Formal Synthesis of Partially-Observable Cyber-Physical Systems

Niloofar Jahanshahi

Dissertation
an der Fakultät Für Mathematik, Informatik und Statistik
der Ludwig–Maximilians–Universität
München

München, 2023

Formal Synthesis of Partially-Observable Cyber-Physical Systems

Niloofar Jahanshahi

Dissertation
an der Fakultät Für Mathematik, Informatik und Statistik
der Ludwig–Maximilians–Universität
München

vorgelegt von
Niloofar Jahanshahi
aus Tehran, Iran

München, den 15/06/2023

Erstgutachter: Prof. Majid Zamani
Zweitgutachter: Prof. Matthias Althoff
Tag der mündlichen Prüfung: 06/09/2023

Eidesstattliche Versicherung

Hiermit erkläre ich, Niloofar Jahanshahi, an Eides statt, dass die vorliegende Dissertation ohne unerlaubte Hilfe gemäß Promotionsordnung vom 12.07.2011, § 8, Abs. 2 Pkt. 5, angefertigt worden ist.

München, 12.06.2023

Niloofar Jahanshahi

Contents

List of Figures

Zusammenfassung

Diese Dissertation ist durch die Herausforderungen motiviert, die sich bei der Synthese von Reglern für teilbeobachtbare cyber-physische Systeme (PO-CPS) ergeben. In den letzten zehn Jahren sind CPS allgegenwärtig und ein integraler Bestandteil unseres täglichen Lebens geworden. Beispiele für solche Systeme reichen von autonomen Fahrzeugen, Drohnen und Flugzeugen bis hin zu Robotern und moderner Fertigung. In vielen Bereichen wird von diesen Systemen erwartet, dass sie komplexe logische Aufgaben erfüllen. Solche Aufgaben können in der Regel mit Formeln der temporalen Logik oder als (un)endliche Zeichenketten über endlichen Automaten ausgedrückt werden. In den letzten Jahren haben sich abstraktionsbasierte Techniken als sehr vielversprechend für die formale Synthese von Steuerungen erwiesen. Da diese Techniken auf der Diskretisierung von Zustands- und Eingabemengen beruhen, leiden sie bei großen Systemen leider stark unter dem Fluch der Dimensionalität, d.h. die Rechenkomplexität wächst exponentiell mit der Dimension der Zustandsmenge. Um den großen Rechenaufwand zu überwinden, hat ein diskretisierungsfreier Ansatz, der auf Kontroll-Barriere-Funktionen basiert, großes Potenzial zur Lösung formaler Syntheseprobleme gezeigt. In dieser Dissertation wird ein systematischer Ansatz zur Synthese einer hybriden Kontrollregel für teilweise beobachtbare (stochastische) Regler ohne Diskretisierung der Zustandsmengen vorgestellt.

In vielen realen Anwendungen sind vollständige Zustandsinformationen nicht immer verfügbar (aufgrund der Kosten für die Erfassung oder der Nichtverfügbarkeit der Messungen). Daher betrachten wir in dieser Dissertation teilweise beobachtbare (stochastische) Regler. Unter der Voraussetzung geeigneter Zustandsschätzer ist es unser Ziel, einen Konzept von Kontroll-Barriere-Funktionenzu verwenden, um Kontrollregeln zu synthetisieren, die eine untere Schranke für die Wahrscheinlichkeit liefern (und möglicherweise maximieren), dass die Trajektorien des teilweise beobachtbaren (stochastischen) Kontrollsystems komplexe logische Spezifikationen wie Sicherheit und solche, die als deterministische endliche Automaten (DFA) ausgedrückt werden können, erfüllen. In dieser Dissertation werden zwei Hauptansätze zur Konstruktion von Kontroll-Barriere-Funktionenvorgestellt. Beim ersten Ansatz ist kein Vorwissen über die Schätzgenauigkeit erforderlich. Der zweite Ansatz verwendet eine (Wahrscheinlichkeits-)Grenze für die Schätzgenauigkeit.

Obwohl das Syntheseverfahren für niedrigdimensionale Systeme an sich schon eine Herausforderung darstellt, ist die Aufgabe für große zusammenhängende Systeme sehr viel rechenintensiver (wenn nicht gar unmöglich). Um die Herausforderungen zu bewältigen, die sich bei großen Systemen ergeben, entwickeln wir Ansätze zur Verringerung des Rechenaufwan-

des. Indem wir ein großes, teilweise beobachtbares Kontrollsystem als eine Verbindung von niederdimensionalen Subsystemen betrachten, berechnen wir sogenannte lokale Kontrollbarrierefunktionen für Subsysteme zusammen mit den entsprechenden lokalen Reglern. Unter der Annahme einiger small-gain Bedingungen nutzen wir dann die lokalen Kontrollbarrierefunktionen der Teilsysteme, um kompositionell eine Gesamtkontrollbarrierefunktion für das gesamte verbundene System zu konstruieren.

Da geschlossene mathematische Modelle für viele physikalische Systeme entweder nicht verfügbar oder zu kompliziert sind, um von Nutzen zu sein, erweitern wir unsere Dissertation auch auf die Synthese von Sicherheitsreglern für teilweise beobachtbare Systeme mit unbekannter Dynamik. Um dieses Problem anzugehen, verwenden wir einen datengesteuerten Ansatz und konstruieren Kontroll-Barriere-Funktionenund ihre entsprechenden Regler anhand von Datensätzen, die aus den Trajektoren der Ausgangswerte der Systeme und den Trajektorien der Schätzer gesammelt wurden.

Um die Wirksamkeit der in dieser Dissertation vorgeschlagenen Ergebnisse zu demonstrieren, betrachten wir verschiedene Fallstudien, wie z.B. einen Gleichstrommotor, ein adaptives Geschwindigkeitsregelungssystem (ACC), das aus Fahrzeugen in einem Zug besteht, und ein Moore-Greitzer-Triebwerksmodell.

Abstract

This dissertation is motivated by the challenges arising in the synthesis of controllers for partially-observable cyber-physical systems (PO-CPSs). In the past decade, CPSs have become ubiquitous and an integral part of our daily lives. Examples of such systems range from autonomous vehicles, drones, and aircraft to robots and advanced manufacturing. In many applications, these systems are expected to do complex logic tasks. Such tasks can usually be expressed using temporal logic formulae or as (in)finite strings over finite automata. In the past few years, abstraction-based techniques have been very promising for the formal synthesis of controllers. Since these techniques are based on the discretization of state and input sets, when dealing with large-scale systems, unfortunately, they suffer severely from the curse of dimensionality (*i.e.*, the computational complexity grows exponentially with the dimension of the state set). In order to overcome the large computational burden, a discretization-free approach based on *control barrier functions* has shown great potential to solve formal synthesis problems. In this thesis, we provide a systematic approach to synthesize a hybrid control policy for partially-observable (stochastic) control systems without discretizing the state sets.

In many real-life applications, full-state information is not always available (due to the cost of sensing or the unavailability of the measurements). Therefore, in this thesis, we consider partially-observable (stochastic) control systems. Given proper state estimators, our goal is to utilize a notion of control barrier functions to synthesize control policies that provide (and potentially maximize) a lower bound on the probability that the trajectories of the partially-observable (stochastic) control system satisfy complex logic specifications such as safety and those that can be expressed as deterministic finite automata (DFA). Two main approaches are presented in this thesis to construct control barrier functions. In the first approach, no prior knowledge of estimation accuracy is needed. The second approach utilizes a (probability) bound on the estimation accuracy.

Though the synthesis procedure for lower-dimensional systems is challenging itself, the task is much more computationally expensive (if not impossible) for large-scale interconnected systems. To overcome the challenges encountered with large-scale systems, we develop approaches to reduce the computational complexity. In particular, by considering a large-scale partially-observable control system as an interconnection of lower-dimensional subsystems, we compute so-called *local control barrier functions* for subsystems along with the corresponding local controllers. By assuming some small-gain type conditions, we then utilize local control barrier functions of subsystems to compositionally construct an overall

control barrier function for the interconnected system.

Finally, since closed-form mathematical models of many physical systems are either unavailable or too complicated to be of any use, we also extend our work to the synthesis of safety controllers for partially-observable systems with unknown dynamics. To tackle this problem, we utilize a data-driven approach and construct control barrier functions and their corresponding controllers via sets of data collected from the output trajectories of the systems and the trajectories of the estimators.

To demonstrate the effectiveness of the proposed results in the thesis, we consider various case studies, such as a DC motor, an adaptive cruise control (ACC) system consisting of vehicles in a platoon, and a Moore-Greitzer jet engine model.

Acknowledgments

I would like to express my sincere gratitude to my supervisor, Prof. Majid Zamani, for providing me the opportunity to work for the doctoral degree and for his wisdom, enthusiasm, and patience throughout my doctoral research. His expertise and insight have been invaluable in shaping my research and personal growth. I would also like to thank my colleagues at the SoSy-Lab, Institute of Informatics at LMU Munich, and the HyConSys Lab, Computer Science Department, University of Colorado Boulder, for their stimulating discussions and helpful feedback. I wish to sincerely thank the research training group ConVeY (DFG GRK 2428) for providing such a conducive research environment. I also wish to thank Prof. Matthias Althoff for being the external examiner for my dissertation. I would also like to highly appreciate my great friends and colleagues, Mahathi Anand and Martin Spiessl, for their unwavering friendship and invaluable assistance. Special thanks to my fiancé, Soheil Ghadiri, for his unwavering love and support, and to my dear friend Sepideh Motevali for her constant encouragement and motivation. Finally, I am deeply grateful to my parents, my brother Behnam, and my aunt Shahin for their love, patience, and understanding, which enabled me to pursue my doctoral studies.

Chapter 1

Introduction

1.1 Motivation and Contributions

Cyber-physical systems (CPSs) consist of sensing, computation, and communication components that collaborate together in order to control a physical entity [1]. This close-knit interaction between communication and computing devices with the physical environment extends human capabilities by allowing for real-time monitoring and control of physical entities. These characteristics make CPSs ideal for use in a wide range of applications, such as autonomous drones, autonomous vehicles, robot-assisted surgery, building management systems, and so on. Figure 1.1 illustrates the use of CPSs.

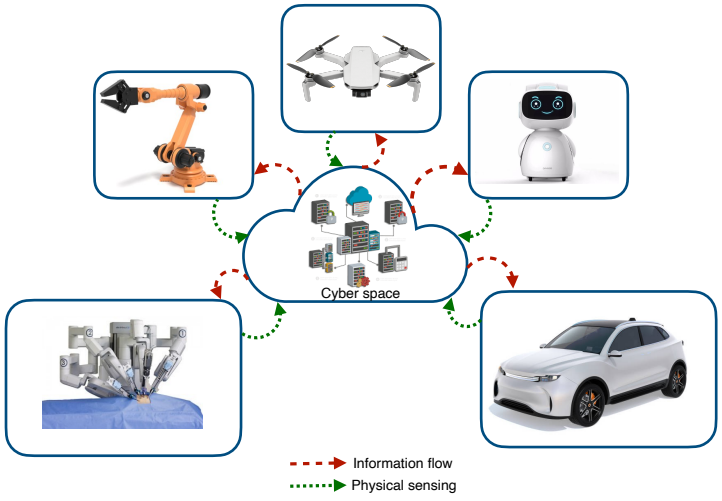

Figure 1.1: Application scenarios of CPSs.

The real-time monitoring and control of physical entities in CPSs is enabled by the presence of feedback control loops. In these feedback control loops, sensors, controllers, and communication networks work together in order to satisfy a property of interest. Figure 1.2 depicts the feedback control loop in CPSs. Due to the increasing complexity

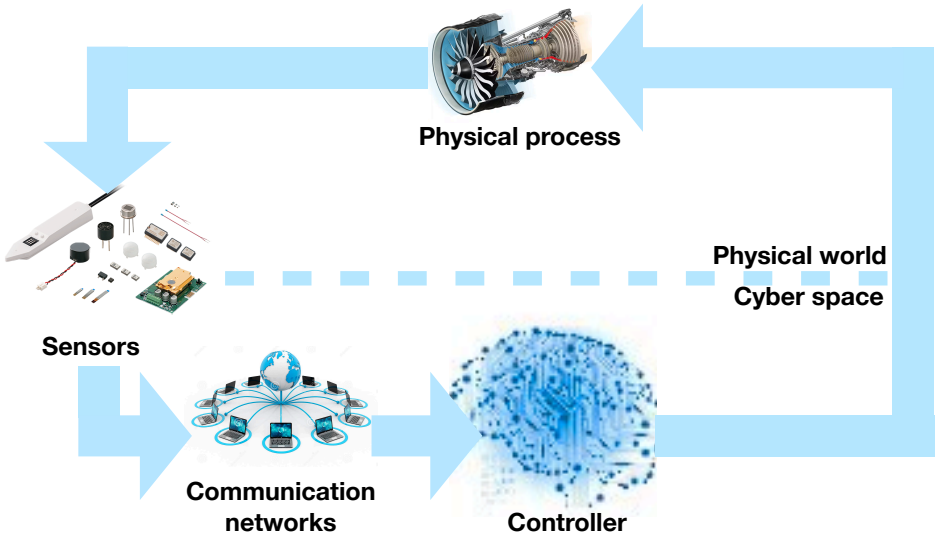

Figure 1.2: Closed-loop interpretations of CPSs.

of CPSs, designing controllers for these systems poses several challenges. Some of these challenges are listed below:

- Stochasticity: CPSs can exhibit stochastic behaviour [2].
- Incomplete or partial information: in many real-world applications, not all of the system's states are measurable due to factors such as low sensor quality, sensor failure, or adverse environmental conditions [1].
- Large system sizes: systems are becoming larger, more complex, and more interconnected [3].
- Complex properties of interests: traditionally, stability was the main concern when synthesizing controllers for CPSs. However, as systems become more complex, the properties of interest go beyond classical stability and robustness. Nowadays, real-world systems are expected to perform complex logic tasks. Such complex tasks can usually be expressed via temporal logic formulae or as (in)finite strings over automata [4].
- Unknown mathematical models: in many cases, the mathematical model of the system is unknown, and developing accurate mathematical models for systems can be too complicated to be of any use [5].

One approach to addressing the above-mentioned challenges and synthesize automated, correct-by-construction controllers is to utilize abstraction-based techniques [6, 7, 8]. Since these techniques are based on the discretization of state and input sets, when dealing with large-scale systems, unfortunately, they suffer severely from the curse of dimensionality (*i.e.*, the computational complexity grows exponentially with the dimension of the state

set). In order to address this issue, compositionality techniques have shown great potential, where formal synthesis for the interconnected system is performed by computing abstractions and controllers for smaller subsystems [9, 10, 11].

Alternatively, another promising method for solving formal synthesis problems is the use of discretization-free approaches based on so-called *control barrier functions*. Control barrier functions (CBFs) are an important class of mathematical functions used to guarantee the safety of a control system by ensuring that it avoids a predefined unsafe region. Particularly, CBFs are useful in synthesizing controllers that satisfy complex logic specifications. The use of CBFs in synthesizing controllers has several advantages. First, it provides a formal and rigorous approach to the controller design process, ensuring that the system remains safe and satisfies the desired specifications. Second, it can handle complex specifications that cannot be satisfied using traditional control design techniques. See the results in [12, 13, 14], and [15] for the synthesis of controllers using CBFs.

Since in many real-life applications, all the system's states are not available, some recent works have investigated controller synthesis problems via CBFs for systems with partial-information. Developing techniques that can handle the case where not all the system states are available will further enhance the applicability of CBFs in real-world applications. To this end, by assuming a priori knowledge of control barrier functions and having an unbounded input set, the results in [16] and [17] synthesize barrier-based controllers for stochastic systems with partial information. In particular, these results require the control barrier functions to exhibit supermartingale property, which presupposes stochastic stability and vanishing noise at the equilibrium point of the system. Moreover, the aforementioned approaches are only applicable to systems with unbounded input sets, and they do not provide any probabilistic guarantee when the input set is bounded.

Motivated by the above results and their limitations, this thesis focuses on developing state-space discretization-free techniques to synthesize controllers for partially-observable (stochastic) control systems. When only partial system information is available, several approaches can be used to estimate the missing information. One common approach is to use state observers or state estimators, which estimate the system's states based on the available measurements. These estimated states can then be used to compute the CBF and its corresponding controller. In this thesis, using proper state estimators, we utilize notions of CBFs to synthesize controllers enforcing complex logic specifications such as safety and those that can be expressed as deterministic finite automata (DFA). In particular, the results provide two approaches for the construction of CBFs. In the first approach, CBFs are constructed over the dynamics of the estimator. This approach requires a priori knowledge of the estimation accuracy. In the second approach, CBFs are defined over augmented systems that include both the systems and their estimators. By doing so, it becomes possible to design CBFs without explicitly requiring the estimation accuracy. This approach can be effective when obtaining the estimation accuracy is challenging or not possible. We also provide a sum-of-squares (SOS) optimization approach to search for those CBFs and, accordingly, compute the corresponding controllers. To address the challenge of scalability arising from the numerical search for CBFs, a compositional approach to construct control barrier functions for large-scale systems is provided. This approach considers the

large-scale system as an interconnected one, consisting of finitely many smaller subsystems, allowing for the design of distributed controllers. Finally, we extend our results to partially-observable systems with unknown dynamics, where control barrier functions and their corresponding controllers are constructed using input-output data collected from the trajectories of the system and its estimator.

1.2 Outline of the Thesis

This dissertation is divided into 7 chapters, the first of which is the current introduction. The remaining are structured as follows.

Chapter 2 contains mathematical notations, preliminaries, and system definitions that will be used throughout the thesis.

Chapter 3 discusses the synthesis of controllers for partially-observable continuous-time stochastic control systems to ensure finite-time safety. Given an estimator with a probabilistic guarantee on the accuracy of the estimation, this chapter proposes an approach to compute a controller together with a lower bound on the probability that the system's trajectories remain safe over a finite time-horizon. Additionally, this chapter presents a method to compute a probability bound on estimator accuracy using stochastic simulation functions.

Chapter 4 focuses on the formal synthesis of controllers for partially-observable continuous-time jump-diffusion systems against complex logic specifications. The proposed approach in this chapter does not require knowledge of estimation accuracy. The synthesized controllers provide lower bounds on the probabilities of the system's trajectories satisfying complex specifications expressed by deterministic finite automata.

Chapter 5 presents a compositional framework for synthesizing safety controllers for networks of partially-observable discrete-time stochastic control systems, also known as POMDPs. In particular, the results in this chapter reduce the computational complexity of the synthesis schemes outlined in Chapters 3 and 4. This approach involves the use of local control barrier functions that are computed for subsystems, which are then used in a compositional manner to construct control barrier functions for POMDPs. The proposed method employs two different strategies for computing local control barrier functions for subsystems. The first strategy, which builds upon the results discussed in Chapter 4, eliminates the need for prior knowledge of estimation accuracy. On the other hand, the second framework incorporates the probability bound on the estimation accuracy by utilizing stochastic simulation functions, as introduced in Chapter 3. Both proposed schemes derive sufficient small-gain type conditions to compositionally construct control barrier functions for interconnected POMDPs using local barrier functions computed for subsystems. The constructed CBFs for the overall networks enable the computation of lower bounds on the probabilities that the interconnected POMDPs avoid certain unsafe regions in finite time horizons.

Chapter 6 provides a data-driven approach for computing polynomial-type controllers that ensure the safety of partially-observable continuous-time polynomial-type systems

with unknown dynamics by leveraging a notion of control barrier functions. The proposed approach only requires a single output trajectory from the system and a single state trajectory from its estimator.

Chapter 7 provides a summary of the results of this dissertation and outlines potential future research directions.

Chapter 2

Mathematical Notations, Preliminaries and Basic Notions in Control Theory

2.1 Notations

The following notations are employed throughout the thesis. The sets of nonnegative and positive integers are denoted by $\mathbb{N} := \{0, 1, 2, \ldots\}$ and $\mathbb{N}_{\geq 1} := \{1, 2, 3, \ldots\}$, respectively. Moreover, the symbols $\mathbb{R}, \mathbb{R}_{>0}$, and $\mathbb{R}_{\geq 0}$ denote, respectively, the sets of real, positive and nonnegative real numbers. We use $\mathbb{R}^n$ to denote an n-dimensional Euclidean space and $\mathbb{R}^{n\times m}$ to denote the space of real matrices with n rows and m columns. Given N vectors $x_i \in \mathbb{R}^{n_i}, n_i \in \mathbb{N}_{\geq 1}$, and $i \in \{1, \ldots, N\}$, we use $[x_1; \ldots; x_n]$ and $[x_1, \ldots, x_n]$ to denote the corresponding column and row vectors, respectively, with dimension $\sum_i n_i$. We denote by $\| \, . \, \|$ and $\| \, . \, \|_2$ the infinity and Euclidean norms, respectively. Given a set X, we denote its ϵ-inflated version by $X^\epsilon := \{\hat{x} \in X \mid \exists x \in X, \|\hat{x} - x\| \leq \epsilon\}$, with $\epsilon \in \mathbb{R}_{>0}$, and by 2^X the power set of X, *i.e.*, the set of all subsets of X. Moreover, we denote the empty set by $\emptyset$ and the diagonal set by Δ_d, where $\Delta_d \subset \mathbb{R}^{2n}$ is defined as $\Delta_d = \{(x, x), x \in \mathbb{R}^n\}$. Given any $a \in \mathbb{R}$, $|a|$ denotes the absolute value of a. Symbols $\mathbf{0}_n$, and $\mathbb{1}_n$ denote the column vector in $\mathbb{R}^{n\times 1}$ with all elements equal to zero and one, respectively. Furthermore, we denote by $e_i \in \mathbb{R}^n$ the vector whose all elements are zero, except the i^{th} element, which is one. We also use $\mathbb{I}_n$ and $\mathbf{0}_{n\times m}$ to denote the identity matrix in $\mathbb{R}^{n\times n}$ and the zero matrix in $\mathbb{R}^{n\times m}$, respectively. The identity function and composition of functions are denoted by $\mathcal{I}_d$ and the symbol $\circ$, respectively.

Given a matrix $M \in \mathbb{R}^{n\times n}$, $\mathrm{Tr}(M)$ represents trace of M which is the sum of all diagonal elements of M. A symmetric matrix $P \in \mathbb{R}^{n\times n}$ is said to be positive definite, denoted by $P \succ 0$, if all its eigenvalues are positive. We also use $\lambda_{\min}(P)$ to represent the minimum eigenvalue of the symmetric matrix P. Given sets X and Y, we denote $f : X \to Y$ an ordinary map from X to Y and the notation $|X|$ denotes the cardinality of set X. Given functions $f_i : X_i \to Y_i$, for any $i \in \{1, \ldots, N\}$, their Cartesian product

$\prod_{i=1}^{N} f_i : \prod_{i=1}^{N} X_i \to \prod_{i=1}^{N} Y_i$ is defined as $(\prod_{i=1}^{N} f_i)(x_1, \ldots, x_N) = [f_1(x_1); \ldots; f_N(x_N)]$. We define an indicator function $\mathbf{I}_{\mathscr{A}}(x) : X \to \{0, 1\}$, where $\mathbf{I}_{\mathscr{A}}(x) := 1$ if $x \in \mathscr{A} \subseteq X$, and $\mathbf{I}_{\mathscr{A}}(x) := 0$ otherwise. A function $\kappa : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$, is said to be a class $\mathcal{K}$ function if it is continuous, strictly increasing, and $\kappa(0) = 0$. A class $\mathcal{K}$ function $\kappa(\cdot)$ is said to be a class $\mathcal{K}_\infty$ if $\kappa(r) \to \infty$ as $r \to \infty$.

2.2 Preliminaries

We consider a probability space $(\Omega, \mathcal{F}_\Omega, \mathbb{P}_\Omega)$, where Ω is a sample space, $\mathcal{F}_\Omega$ is a sigma-algebra on Ω, and $\mathbb{P}_\Omega$ is a probability measure that assigns probabilities to events. We assume that the triple $(\Omega, \mathcal{F}_\Omega, \mathbb{P}_\Omega)$ is endowed with a filtration $\mathbb{F} = (\mathcal{F}_s)_{s \geq 0}$ satisfying the usual conditions of right continuity and completeness [18]. Moreover, we consider $(W_{ks})_{s \geq 0}$ as a $\bar{r}_k$-dimensional $\mathbb{F}$-Brownian motions, $k = 1, 2$, and $(P_{ks})_{s \geq 0}$ as a $\bar{q}_k$-dimensional $\mathbb{F}$-Poisson processes, with $k = 1, 2$. We assume that the Poisson processes and Brownian motions are independent of each other. The Poisson process $P_{ks} := [P_{ks}^1; \cdots; P_{ks}^{\bar{q}_k}]$ models $\bar{q}_k$ kinds of events, $k = 1, 2$, whose occurrences are assumed to be independent of each other.

We assume that random variables introduced in this thesis are measurable functions of the form $X : (\Omega, \mathcal{F}_\Omega) \to (\mathcal{S}_X, \mathcal{F}_X)$. Any random variable X induces a probability measure on its space $(\mathcal{S}_X, \mathcal{F}_X)$ as $Prob\{A\} = \mathbb{P}_\Omega\{X^{-1}(A)\}$ for any $A \in \mathcal{F}_X$. We often directly discuss the probability measure on $(\mathcal{S}_X, \mathcal{F}_X)$ without explicitly mentioning the underlying probability space and the function X itself. We call a topological space $\mathcal{S}$ a Borel space if it is homeomorphic to a Borel subset of a Polish space (*i.e.,* a separable and completely metrizable space). Examples of a Borel space are the Euclidean space $\mathbb{R}^n$ and its Borel subsets endowed with a subspace topology, as well as hybrid spaces. A Borel sigma-algebra is denoted by $\mathfrak{B}(\mathcal{S})$, where any Borel space $\mathcal{S}$ is assumed to be endowed with it. A map $f : \mathcal{S} \to Y$ is measurable whenever it is Borel measurable.

2.3 System Definitions

In this section, we define different forms of partially-observable control systems that are considered throughout this thesis.

2.3.1 Partially-Observable Continuous-Time Stochastic Control Systems

The formal definition of partially-observable continuous-time stochastic control systems is given as follows.

Definition 1. *A partially-observable continuous-time stochastic control system (PO-ct-SCS) is a tuple* $\mathcal{S}_S = (\mathbb{R}^n, \mathbb{R}^m, U, f, g_1, \mathbb{R}^p, h, g_2)$*, where*

- $\mathbb{R}^n$ *is the state space;*
- $\mathbb{R}^m$ *is the input space;*
- U *is a subset of all* $\mathbb{F}$*-progressively measurable processes with values in* $\mathbb{R}^m$*, (see [19]);*
- $f : \mathbb{R}^n \times \mathbb{R}^m \to \mathbb{R}^n$ *satisfies the following Lipschitz assumption: there exist constants* $L_x, L_u \in \mathbb{R}_{\geq 0}$ *such that* $\|f(x,u) - f(x',u')\|_2 \leq L_x\|x - x'\|_2 + L_u\|u - u'\|_2$, $\forall x, x' \in \mathbb{R}^n$ *and* $\forall u, u' \in \mathbb{R}^m$*;*
- $g_1 : \mathbb{R}^n \to \mathbb{R}^{n \times \bar{r}_1}$ *satisfies the following Lipschitz assumption: there exists a constant* $L_{g_1} \in \mathbb{R}_{\geq 0}$ *such that* $\|g_1(x) - g_1(x')\|_2 \leq L_{g_1}\|x - x'\|_2,\ \forall x, x' \in \mathbb{R}^n$*;*
- $\mathbb{R}^p$ *is the output space;*
- $h : \mathbb{R}^n \to \mathbb{R}^p$ *satisfies the following Lipschitz assumption: there exists a constant* $L_h \in \mathbb{R}_{\geq 0}$ *such that* $\|h(x) - h(x')\|_2 \leq L_h\|x - x'\|_2,\ \forall x, x' \in \mathbb{R}^n$*;*
- $g_2 : \mathbb{R}^n \to \mathbb{R}^{p \times \bar{r}_2}$ *satisfies the following Lipschitz assumption: there exists a constant* $L_{g_2} \in \mathbb{R}_{\geq 0}$ *such that* $\|g_2(x) - g_2(x')\|_2 \leq L_{g_2}\|x - x'\|_2,\ \forall x, x' \in \mathbb{R}^n$*.*

A stochastic process $\xi : \Omega \times \mathbb{R}_{\geq 0} \to \mathbb{R}^n$ is said to be a *solution process* of $\mathcal{S}_S$ if there exists $\upsilon \in U$ satisfying the stochastic differential equations (SDE)

$$\mathcal{S}_S : \begin{cases} \mathrm{d}\,\xi &= f(\xi, \upsilon)\,\mathrm{d}\,t + g_1(\xi)\,\mathrm{d}\,W_{1t}, \\ \mathrm{d}\,y &= h(\xi)\,\mathrm{d}\,t + g_2(\xi)\,\mathrm{d}\,W_{2t}, \end{cases} \tag{2.3.1}$$

where $y(t)$ taking values in $\mathbb{R}^p$ denotes the output of $\mathcal{S}_S$ and represents the noisy partial information at each time $t \in \mathbb{R}_{\geq 0}$ $\mathbb{P}$-almost surely ($\mathbb{P}$-a.s.). Solution process of $\mathcal{S}_S$ exists and is unique due to the assumptions on f and g_1 [18]. We assume that the pair $(\frac{\partial f}{\partial x}(x,u), h(x))$ is uniformly detectable [16, Definition 6]. For a PO-ct-SCS $\mathcal{S}_S$ in (2.3.1), we use the notation $\xi_{x_0\upsilon}(t)$ to denote the value of the solution process at time $t \in \mathbb{R}_{\geq 0}$ under the input signal υ starting from the initial state $\xi_{x_0\upsilon}(0) = x_0$ $\mathbb{P}$-a.s., in which x_0 is a random variable that is measurable in $\mathcal{F}_0$.

2.3.2 Partially-Observable Continuous-Time Jump-Diffusion Systems

In some part of this thesis, we consider partially-observable continuous-time jump-diffusion systems formally defined as follows.

Definition 2. *A partially-observable jump-diffusion system (po-JDS), denoted by* $\mathcal{S}_J$*, is described by the following stochastic differential equations (SDE)*

$$\mathcal{S}_J : \begin{cases} \mathrm{d}\,\xi &= f(\xi, \upsilon)\,\mathrm{d}\,t + g_1(\xi)\,\mathrm{d}\,W_{1t} + r_1(\xi)\,\mathrm{d}\,P_{1t}, \\ \mathrm{d}\,y &= h(\xi)\,\mathrm{d}\,t + g_2(\xi)\,\mathrm{d}\,W_{2t} + r_2(\xi)\,\mathrm{d}\,P_{2t}, \end{cases} \tag{2.3.2}$$

where $\xi(t) \in X \subseteq \mathbb{R}^n$ is the value of solution process ξ of $\mathcal{S}_J$, $\upsilon(t) \in U \subseteq \mathbb{R}^m$ is the input vector, and $y(t) \in \mathbb{R}^p$ is the output vector representing the noisy partial observation at time $t \in \mathbb{R}^{\geq}$ $\mathbb{P}$-almost surely ($\mathbb{P}$-a.s.). Functions $f : X \times U \to \mathbb{R}^n$, $g_1 : X \to \mathbb{R}^{n \times \bar{r}_1}$, $g_2 : X \to \mathbb{R}^{p \times \bar{r}_2}$, $r_1 : X \to \mathbb{R}^{n \times \bar{q}_1}$, $r_2 : X \to \mathbb{R}^{p \times \bar{q}_2}$, and $h : X \to \mathbb{R}^p$ are assumed to be Lipschitz continuous to ensure existence and uniqueness of the solution of $\mathcal{S}_J$ [20]. For the PO-JDS $\mathcal{S}_J$ in (2.3.2), we use the notation $\xi_{x_0\upsilon}(t)$ to denote the value of the solution process of $\mathcal{S}_J$ at time $t \in \mathbb{R}_{\geq 0}$ under the input signal υ starting from the initial state $\xi_{x_0\upsilon}(0) = x_0$ $\mathbb{P}$-a.s., in which x_0 is a random variable that is measurable in $\mathcal{F}_0$. We assume that the Poisson processes P^i_{ks} for any $i \in \{1, \ldots, \bar{q}_k\}$, $k = 1, 2$, have the rates of λ_{ki}.

2.3.3 Partially-Observable Continuous-Time Polynomial-Type Systems

A partially-observable continuous-time polynomial-type systems is formalized in the following definition.

Definition 3. *A partially-observable continuous-time polynomial-type system (PO-ct-PS) is described by*

$$\mathcal{S}_P : \begin{cases} \dot{x} = \mathcal{A}\mathcal{M}(x) + \mathcal{B}u, \\ y = \mathcal{C}\mathcal{M}(x), \end{cases} \tag{2.3.3}$$

where $\mathcal{A} \in \mathbb{R}^{n \times N}, \mathcal{B} \in \mathbb{R}^{n \times m}$, and $\mathcal{C} \in \mathbb{R}^{p \times N}$. The vector function $\mathcal{M}(x) \in \mathbb{R}^N$ contains monomials in state $x \in X$, with $X \subset \mathbb{R}^n$ being the state set. Furthermore, $u \in U$ is the control input with input set $U \subset \mathbb{R}^m$, and $y \in Y$ is the output with output set $Y \subset \mathbb{R}^p$. For the PO-ct-PS (2.3.3), we employ notation $x_{x_0\upsilon}$ to denote the trajectory of $\mathcal{S}_P$ starting from an initial state $x_0 = x(0)$, under an input υ, and $x_{x_0\upsilon}(t)$ denotes the value of this trajectory at time $t \in \mathbb{R}_{\geq 0}$.

2.3.4 Partially-Observable Discrete-Time Stochastic Control Systems

In some part of this thesis, we consider partially-observable discrete-time stochastic control systems as formalized in the following definition.

Definition 4. *A partially-observable discrete-time stochastic control system (PO-dt-SCS) is characterized by the tuple*

$$\Sigma_S = (X, U, W, \varsigma_1, f, Y_1, Y_2, h_1, h_2, \varsigma_2), \tag{2.3.4}$$

where,

- *$X \subseteq \mathbb{R}^n$ is a Borel space as the state space of the system. The measurable space with $\mathfrak{B}(X)$ being the Borel sigma-algebra on the state space is denoted by $(X, \mathfrak{B}(X))$;*
- *$U \subseteq \mathbb{R}^m$ is a Borel space as the* external *input space of the system;*

- $W \subseteq \mathbb{R}^p$ *is a Borel space as the* internal *input space of the system;*
- ς_i, $i \in \{1, 2\}$, *denote sequences of independent and identically distributed* (*i.i.d.*) *random variables from a sample space* Ω *to the uncertainty set* $\mathcal{V}_{\varsigma_i}$,
$$\varsigma_i = \{\varsigma_i(k) : \Omega \to \mathcal{V}_{\varsigma_i}, k \in \mathbb{N}\},$$
- $f : X \times U \times W \times \mathcal{V}_{\varsigma_1} \to X$ *is a measurable function characterizing the state evolution of the system;*
- $Y_1 \subseteq \mathbb{R}^p$ *is a Borel space as the internal output space of the system;*
- $Y_2 \subseteq \mathbb{R}^q$ *is a Borel space as the external output space of the system;*
- $h_1 : X \to Y_1$ *is a measurable function that maps a state* $x \in X$ *to its internal output* $y_1 = h_1(x)$*;*
- $h_2 : X \times \mathcal{V}_{\varsigma_2} \to Y_2$ *is a measurable function that maps a state* $x(k) \in X$ *to its external output* $y_2(k) = h_2(x(k), \varsigma_2(k))$.

An evolution of the state of PO-dt-SCS Σ_S and its output for given input sequences $\upsilon(\cdot) : \mathbb{N} \to U$ and $w(\cdot) : \mathbb{N} \to W$ are described by

$$\Sigma_S : \begin{cases} x(k+1) = f(x(k), \upsilon(k), w(k), \varsigma_1(k)), \\ y_1(k) = h_1(x(k)), \\ y_2(k) = h_2(x(k), \varsigma_2(k)), \qquad k \in \mathbb{N}. \end{cases} \tag{2.3.5}$$

A PO-dt-SCS Σ_S in (2.3.4) can be *equivalently* represented as a partially-observable Markov decision process (POMDP) [21]. Hence, we interchangeably employ terms PO-dt-SCS and POMDP in the thesis.

We associate to U and W sets $\mathcal{U}$ and $\mathcal{W}$, respectively, to be collections of sequences $\{\upsilon(k) : \Omega \to U, k \in \mathbb{N}\}$ and $\{w(k) : \Omega \to W, k \in \mathbb{N}\}$, in which $\upsilon(k)$ and $w(k)$ are independent of $\varsigma_i(l)$ for any $k, l \in \mathbb{N}$, $l \geq k$ and $i \in \{1, 2\}$. The random sequences $x_{x_0 \upsilon w} : \Omega \times \mathbb{N} \to X$, $y_{1_{x_0 \upsilon w}} : \Omega \times \mathbb{N} \to Y_1$, and $y_{2_{x_0 \upsilon w}} : \Omega \times \mathbb{N} \to Y_2$ satisfying (2.3.5) are called respectively the *solution process*, *internal output* and *external output processes* of Σ_S, respectively, under an external input υ, an internal input w, and an initial state x_0. The external output signal y_1 and the internal input signal w represent the interconnections between subsystems, where y_1 is the information that each subsystem sends to its neighbouring subsystems and w is the information fed to each subsystem by its neighbours.

In this thesis, we are ultimately interested in investigating networks of systems. In this case, the tuple representing interconnected systems, not containing internal inputs and outputs, is $\Sigma_S = (X, U, \varsigma_1, f, Y, h, \varsigma_2)$, where $f : X \times U \times \mathcal{V}_{\varsigma_1} \to X$, and

$$\Sigma_S : \begin{cases} x(k+1) = f(x(k), \upsilon(k), \varsigma_1(k)), \\ y(k) = h(x(k), \varsigma_2(k)), \qquad k \in \mathbb{N}. \end{cases} \tag{2.3.6}$$

Note that in this thesis, with a slight abuse of notation, we use the same naming in both continuous and discrete time, but the distinction will be clear from the context.

Chapter 3

Controller Synthesis for Partially-Observable Stochastic Control Systems

This chapter deals with the problem of synthesizing controllers for partially-observable stochastic control systems to ensure finite-time safety. Given an estimator with a probabilistic guarantee on the accuracy of the estimations, we provide an approach to compute a controller providing a lower bound on the probability that the trajectories of the stochastic control system remain safe over a finite time-horizon. To obtain such controllers, we utilize a notion of control barrier functions. We also provide an approach to compute a probability bound on estimator accuracy by using a notion of so-called stochastic simulation function.

3.1 Introduction

Stochastic control systems are becoming ubiquitous and an integral part of our daily lives. Examples of such systems range from robots and medical devices to smart grids and automotive networks. Safety is an important design objective for many of these control systems. Failure to ensure safety could result in loss of life or damage to the system and the environment. For this reason, formal verification and synthesis of controllers against safety specifications has gained considerable attention among both control theorists and computer scientists. In principle, safety verifications' goal is to show that the systems' trajectories will not enter an unsafe region in the state space. In the context of partially-observable stochastic control systems, ensuring safety becomes an even more challenging task. Partial-observability is a common characteristic in many real-world systems, where only a subset of the system's states can be directly measured or observed. This limited information poses challenges in system analysis and control design, requiring techniques like state estimation to estimate the unobservable states.

3.1.1 Related Literature

Abstraction-based techniques, which are based on the discretization of state and input sets, have become quite popular for the formal synthesis of controllers [6, 7, 22]. However, the major bottleneck of these techniques is that they suffer severely from the curse of dimensionality, where the computational complexity grows exponentially with the dimension of the state set.

On the other hand, discretization-free approaches using *barrier functions* have shown potential for solving verification or synthesis of deterministic and stochastic systems against safety specifications (see [12, 23, 24] for deterministic systems and [13, 15, 25, 26] for stochastic systems). These functions are defined over the state space of the system and have to satisfy a set of inequalities defined over the function itself and the one step transition of the system. The existence of such a function provides directly the controller together with a guarantee on the satisfaction of the safety specification.

However, all the aforementioned results assume the availability of full state information, which is not the case in many real-world applications. This limitation led to new challenges in the synthesis of controllers for systems with partial or incomplete information. Motivated by these challenges, the proposed approaches in [17] and [16] provide infinite-time horizon guarantees for the safety of the system with probability 1 while assuming a prior knowledge of control barrier functions and considering an unbounded input set. However, in order to provide infinite time horizon guarantees, they require that the control barrier functions exhibit supermartingale property, which presupposes stochastic stability and vanishing noise at the equilibrium point of the system. The problem of synthesizing safety controllers for partially-observable Markov decision processes (POMDPs) using barrier functions has also been studied in [27].

3.1.2 Contributions

The contents of this chapter have been published in the IFAC World Congress [28]. It is a joint work with Prof. Pushpak Jagtap and Prof. Majid Zamani. The author of the thesis has established the results and written the draft. Pushpak Jagtap contributed to the initial discussions, the results, the revision of the draft, and mentoring. Majid Zamani supervised the work.

In this chapter, we consider the problem of formal synthesis of continuous-time stochastic control systems with partial state information ensuring safety specification over a finite-time horizon *without* requiring any assumptions on the stability of the stochastic system. In order to achieve this, we do not require the supermartingale property on control barrier functions. In our setting, we only require that control barrier functions exhibit a c-martingale property, which is a relaxation of the supermartingale one. Remark that a supermartingale property often presupposes stochastic stability and vanishing noise at the equilibrium point, which are not the case for the c-martingale property. Hence, finding c-martingale barrier functions is much easier than finding supermartingale ones. On the other hand, requiring only c-martingale property comes at the cost of providing a guaran-

tee for only finite time horizon, whereas the supermartingale property provides an infinite time horizon guarantee.

Our main contribution is to provide a systematic approach for computing a lower bound on the probability that the stochastic control system with partial information satisfies safety specifications over a finite-time horizon. Given an appropriate estimator with a probabilistic guarantee on the closeness of the estimator's and system's trajectories, we provide sufficient conditions for control barrier functions under which one can provide the lower bound on the probability of satisfying safety specifications over a finite time-horizon. Then, we provide sufficient conditions for computing control barrier functions and corresponding controllers. We also provide an approach to compute probability bound on the estimator accuracy for a class of stochastic control systems by utilizing a notion of so-called stochastic simulation function ([29, 30]).

3.2 Preliminaries and Problem Definition

In order to synthesize safety controllers for PO-ct-SCSs as in (2.3.1), we first raise the following assumption on the existence of the estimator that estimates the state of the PO-ct-SCS $\mathcal{S}_S$ as in (2.3.1) with a probabilistic guarantee on the estimation accuracy.

Assumption 1. *The states of the PO-ct-SCS $\mathcal{S}_S$ in* (2.3.1) *can be estimated by a proper estimator $\widehat{\mathcal{S}}_S$ represented in the form of stochastic differential equation with the estimated state trajectory $\hat{\xi}(t)$ which is described by:*

$$\widehat{\mathcal{S}}_S : \mathrm{d}\,\hat{\xi} = f(\hat{\xi}, \upsilon)\,\mathrm{d}\,t + K\big(\mathrm{d}\,y - h(\hat{\xi})\,\mathrm{d}\,t\big), \tag{3.2.1}$$

where $K \in \mathbb{R}^{n\times p}$ is the estimator gain. Moreover, the probabilistic bound on the accuracy of the estimator is given as [31]:

$$\forall \theta \in (0,1] \quad \exists \epsilon > 0 \quad \textit{such that} \quad \mathbb{P}\Big(\sup_{t\geq 0} \|\xi_{x_0\upsilon}(t) - \hat{\xi}_{\hat{x}_0\upsilon}(t)\|_2 \leq \epsilon\Big) \geq 1-\theta. \tag{3.2.2}$$

To find the relation between ϵ and θ, one can use the notion of so-called *stochastic simulation functions* introduced in [32]. The construction of stochastic simulation functions and the probability bound for the case of linear stochastic control systems is provided in Section 3.4.

For later use, we provide the definition of the infinitesimal generator (denoted by operator $\mathcal{D}$) for the stochastic control system $\mathcal{S}_S$ using Ito's differentiation [18]. Let $\mathcal{B} : \mathbb{R}^n \to \mathbb{R}$ be a twice differentiable function. The infinitesimal generator of $\mathcal{B}$ associated with the system $\mathcal{S}_S$ for all $x \in \mathbb{R}^n$ and for all $u \in U$ is given by

$$\mathcal{D}\mathcal{B}(x,u) = \frac{\partial \mathcal{B}}{\partial x}(x) f(x,u) + \frac{1}{2}\mathrm{Tr}\big(g_1^\top(x)\frac{\partial^2 \mathcal{B}}{\partial x^2}(x) g_1(x)\big). \tag{3.2.3}$$

Now, we formally define the main synthesis problem considered in this chapter.

Problem 5. *Given a partially-observable continuous-time stochastic control system $\mathcal{S}_S$ in* (2.3.1)*, its estimator $\widehat{\mathcal{S}}_s$* (3.2.1) *satisfying* (3.2.2)*, and initial and unsafe sets $X_0 \subset \mathbb{R}^n$, $X_1 \subset \mathbb{R}^n$, respectively, compute a controller (if existing) and a real value $\vartheta \in (0,1)$ such that the probability of the solution process of $\mathcal{S}_S$ starting from X_0 and not reaching X_1 over the finite time horizon $T \in \mathbb{R}_{>0}$ is lower bounded by ϑ, i.e.,*

$$\mathbb{P}\{\forall t \in [0,T),\ \xi_{x_0 v}(t) \notin X_1\} \geq \vartheta, \forall x_0 \in X_0.$$

Finding a solution to Problem 5 (if existing) is difficult in general. In this chapter, we provide a sound method in solving this problem. To synthesize a controller, we utilize the notion of control barrier functions introduced in the next section.

3.3 Control Barrier Functions for PO-ct-SCSs

In this section, we provide sufficient conditions using the so-called control barrier functions under which we can provide the lower bound on the probability that the trajectories of system $\mathcal{S}_S$ start from any initial state in set $X_0 \subset \mathbb{R}^n$ and do not reach unsafe set $X_1 \subset \mathbb{R}^n$. Now, we provide an intermediate result providing an upper bound on the reachability probability for the trajectory of the estimator $\widehat{\mathcal{S}}_S$ in (3.2.1).

Theorem 6. *Consider a PO-ct-SCS $\mathcal{S}_S$ in* (2.3.1)*, an estimator $\widehat{\mathcal{S}}_S$ with the accuracy ϵ as in* (3.2.2)*, and sets $X_0, X_1^\epsilon \subset \mathbb{R}^n$, where X_1^ϵ is the inflated version of X_1. Suppose there exists a twice differentiable function $\mathcal{B} : \mathbb{R}^n \to \mathbb{R}_{\geq 0}$, constants $c \geq 0$ and $\beta_0 \in [0,1)$ such that*

$$\mathcal{B}(\hat{x}) \leq \beta_0 \quad \forall \hat{x} \in X_0, \tag{3.3.1}$$

$$\mathcal{B}(\hat{x}) \geq 1 \quad \forall \hat{x} \in X_1^\epsilon, \tag{3.3.2}$$

$$\inf_{u \in U} \frac{\partial \mathcal{B}}{\partial \hat{x}}(\hat{x}) f(\hat{x},u) + L_h \epsilon \| \frac{\partial \mathcal{B}}{\partial \hat{x}}(\hat{x}) K \|_2 + \frac{1}{2} Tr\Big(g_2^\top(\hat{x}) K^\top \frac{\partial^2 \mathcal{B}}{\partial \hat{x}^2}(\hat{x}) K g_2(\hat{x}) \Big) \leq c \quad \forall \hat{x} \in \mathbb{R}^n, \tag{3.3.3}$$

where $L_h \in \mathbb{R}_{\geq 0}$ is the Lipschitz constant for the function h. Then, the probability that the solution process $\hat{\xi}$ of the estimator $\widehat{\mathcal{S}}_S$ starting from an initial state $\hat{x}_0 \in X_0$ and reaching region X_1^ϵ within time horizon $[0,T) \subset \mathbb{R}_{\geq 0}$ is upper bounded by $\beta_0 + cT$.

Proof. Consider the infinitesimal generator associated with the estimator $\widehat{\mathcal{S}}_S$ as

$$\mathcal{D}\mathcal{B}(\hat{x},u) = \frac{\partial \mathcal{B}}{\partial \hat{x}}(\hat{x}) \Big(f(\hat{x},u) + K\big(h(x) - h(\hat{x})\big) \Big) + \frac{1}{2} \mathrm{Tr}\Big(g_2^\top(\hat{x}) K^\top \frac{\partial^2 \mathcal{B}}{\partial \hat{x}^2}(\hat{x}) K g_2(\hat{x}) \Big).$$

If $\|x - \hat{x}\|_2 \leq \epsilon$, then one gets

$$\frac{\partial \mathcal{B}}{\partial \hat{x}}(\hat{x}) K\big(h(x) - h(\hat{x})\big) \leq \| \frac{\partial \mathcal{B}}{\partial \hat{x}}(\hat{x}) K \|_2 \| h(x) - h(\hat{x}) \|_2 \leq \| \frac{\partial \mathcal{B}}{\partial \hat{x}}(\hat{x}) K \|_2 L_h \epsilon.$$

Hence, if (3.3.3) holds, then

$$\inf_{u\in U} \frac{\partial \mathcal{B}}{\partial \hat{x}}(\hat{x})\Big(f(\hat{x},u) + K\big(h(x)-h(\hat{x})\big)\Big) + \frac{1}{2}\mathrm{Tr}\Big(g_2^\top(\hat{x})K^\top \frac{\partial^2 \mathcal{B}}{\partial \hat{x}^2}(\hat{x})Kg_2(\hat{x})\Big)$$
$$\leq \inf_{u\in U} \frac{\partial \mathcal{B}}{\partial \hat{x}}(\hat{x})f(\hat{x},u) + L_h\epsilon\|\frac{\partial \mathcal{B}}{\partial \hat{x}}(\hat{x})K\|_2 + \frac{1}{2}\mathrm{Tr}\Big(g_2^\top(\hat{x})K^\top \frac{\partial^2 \mathcal{B}}{\partial \hat{x}^2}(\hat{x})Kg_2(\hat{x})\Big) \leq c.$$

Thus, one has $\inf_{u\in U} \mathcal{DB}(\hat{x},u) \leq c$. Now by utilizing [33, Theorem 1], (3.3.1), and the fact that $X_1^\epsilon \subseteq \{\hat{x}\in\mathbb{R}^n \mid \mathcal{B}(\hat{x})\geq 1\}$, we have $\mathbb{P}\{\hat{\xi}_{\hat{x}_0 v}(t)\in X_1^\epsilon \text{ for some } 0\leq t<T \mid \hat{\xi}_{\hat{x}_0 v}(0)=\hat{x}_0\} \leq \mathbb{P}\{\sup_{0\leq t<T}\mathcal{B}(\hat{\xi}_{\hat{x}_0 v}(t))\geq 1 \mid \hat{\xi}_{\hat{x}_0 v}(0)=\hat{x}_0\} \leq \mathcal{B}(\hat{x}_0)+cT \leq \beta_0+cT$ which concludes the proof. □

The function $\mathcal{B}$ in Theorem 6 satisfying (3.3.1) - (3.3.3) is usually referred to as the control barrier function for $\widehat{\mathcal{S}}_S$.

Remark 7. *The above theorem gives controller as the infimum over u of the left-hand side of inequality* (3.3.3)*.*

The result of Theorem 6 guarantees that the following inequality holds:

$$\mathbb{P}\Big\{\exists t\in[0,T),\ \hat{\xi}_{\hat{x}_0 v}(t)\in X_1^\epsilon\Big\} \leq \beta_0 + Tc, \tag{3.3.4}$$

In the next theorem, we provide the upper bound on the reachability property over the trajectory of the original system $\mathcal{S}_S$ by utilizing the bound obtained in Theorem 6 and the estimator accuracy.

Theorem 8. *Consider a PO-ct-SCS $\mathcal{S}_S$ in* (2.3.1)*, an estimator $\widehat{\mathcal{S}}_S$ with the accuracy ϵ as in* (3.2.2)*, the results in Theorem 6, and sets $X_0, X_1, X_1^\epsilon \subset \mathbb{R}^n$. Then for any $x_0\in X_0$*

$$\mathbb{P}\Big\{\exists t\in[0,T),\ \xi_{x_0 v}(t)\in X_1\Big\} \leq \beta_0 + Tc + \theta - \theta(\beta_0+Tc). \tag{3.3.5}$$

Proof. The proof is inspired by the proof of Corollary 3.5 in [34]. Given $x_0, \hat{x}_0 \in X_0$, let us define the events $A_1 := \{\exists t\in[0,T),\ \xi_{x_0 v}(t)\in X_1\}$, $A_2 := \{\exists t\in[0,T),\ \hat{\xi}_{\hat{x}_0 v}(t)\in X_1^\epsilon\}$, and $A_3 := \{\sup_{t\geq 0}\|\xi_{x_0 v}(t)-\hat{\xi}_{\hat{x}_0 v}(t)\|_2 \leq \epsilon\}$. Then, we have

$$\mathbb{P}\{\bar{A}_1\} \overset{(*)}{=} \mathbb{P}\{\bar{A}_2\cap A_3\} = \mathbb{P}\{\bar{A}_2\}\mathbb{P}\{A_3\} \overset{(**)}{\geq} (1-\beta_0-Tc)(1-\theta),$$

where $\bar{A}_i$ is the complement of event A_i for $i\in\{1,2\}$. The first equality $(*)$ comes from the definition of X_1^ϵ being an $\epsilon-$inflated version of X_1. Notice that in the inequality $(**)$, the term $\mathbb{P}\{\bar{A}_2\}$ is lower bounded by $(1-\beta_0-Tc)$. Furthermore, according to (3.2.2), the term $\mathbb{P}\{A_3\}$ is lower bounded by $(1-\theta)$. Thus, one can conclude

$$\mathbb{P}\{A_1\} \leq \beta_0 + Tc + \theta - \theta(\beta_0+Tc).$$

This concludes the proof. □

Corollary 9. *Given the results in Theorem 8, the probability that the trajectories of $\mathcal{S}_S$ start from any $x_0\in X_0$ and stay in $\mathbb{R}^n\setminus X_1$ is lower bounded by*

$$\mathbb{P}\Big\{\forall t\in[0,T),\ \xi_{x_0 v}(t)\notin X_1\Big\} \geq (1-\beta_0-Tc)(1-\theta). \tag{3.3.6}$$

3.3.1 Computation of Control Barrier Functions

Proving the existence of a control barrier function and finding one are in general hard problems. However, one can search for parametric barrier functions of the form $\mathcal{B}(\bar{q}, \hat{x}) = \sum_{i=1}^{\mathsf{r}_b} \bar{q}_i b_i(\hat{x})$ with some user-defined (possibly nonlinear) basis functions $b_i(\hat{x})$ and unknown coefficients $\bar{q}_i \in \mathbb{R}$, $i \in \{1, 2, \ldots, \mathsf{r}_b\}$, and the parametric state feedback controller of the similar form. The following lemma provides a set of sufficient conditions for the existence of such a parametric control barrier function required in Theorem 6, which can be solved as an optimization problem.

Lemma 10. *Consider compact sets X_0, X_1^ϵ, $X_1 \subset \mathbb{R}^n$ as given in Theorem 6. Suppose there exists a parametric function $\mathcal{B}(\bar{q}, \hat{x})$ and parametric functions $\psi_{u_i}(d_{u_i}, \hat{x})$ corresponding to the i^{th} input in $u = (u_1, u_2, \ldots, u_m) \in U \subset \mathbb{R}^m$ with vectors of parameters $\bar{q}$ and d_{u_i} of appropriate sizes, respectively, constants $c \geq 0$ and $\beta_0 \in [0, 1)$ that satisfy*

$$\mathcal{B}(\bar{q}, \hat{x}) \geq 0 \quad \forall \hat{x} \in \mathbb{R}^n, \tag{3.3.7}$$

$$\mathcal{B}(\bar{q}, \hat{x}) \leq \beta_0 \quad \forall \hat{x} \in X_0, \tag{3.3.8}$$

$$\mathcal{B}(\bar{q}, \hat{x}) \geq 1 \quad \forall \hat{x} \in X_1^\epsilon, \tag{3.3.9}$$

$$\begin{aligned} &\frac{\partial \mathcal{B}}{\partial \hat{x}}(\bar{q}, \hat{x}) f(\hat{x}, u) + L_h \epsilon \| \frac{\partial \mathcal{B}}{\partial \hat{x}}(\bar{q}, \hat{x}) K \|_2 + \sum_{i=1}^{m} (u_i - \psi_{u_i}(d_{u_i}, \hat{x})) \\ &+ \frac{1}{2} Tr\Big(g_2^\top(\hat{x}) K^\top \frac{\partial^2 \mathcal{B}}{\partial \hat{x}^2}(\bar{q}, \hat{x}) K g_2(\hat{x}) \Big) \leq c \quad \forall \hat{x} \in \mathbb{R}^n, \forall u \in U. \end{aligned} \tag{3.3.10}$$

Then $\mathcal{B}(\bar{q}, \hat{x})$ satisfies conditions in Theorem 6 and $u_i = \psi_{u_i}(d_{u_i}, \hat{x})$ is the corresponding controller.

Proof. The first three conditions implies (3.3.1) and (3.3.2) along with non-negativeness of the function $\mathcal{B}$. Now, if we choose control input $u_i = \psi_{u_i}(d_{u_i}, \hat{x})$, condition (3.3.10) implies (3.3.3) in Theorem 6 which concludes the proof. □

In order to search for the parameters $\bar{q}$ and d_{u_i} in Lemma 10 satisfying (3.3.7)-(3.3.10), one can use existing nonlinear optimization solvers such as [35]. Note that, the methods may run into local optima, however, one can utilize multi-start techniques [36] to obtain global optima. For the final rigorous verification step, one can use tools such as dReal [37] or RSolver [38] to formally verify that the computed functions indeed satisfy the required conditions.
In order to compute θ in (3.3.6), we utilize the notion of stochastic simulation function which is introduced in the next section.

3.4 Stochastic Simulation Functions

In this section, we define a notion of stochastic simulation functions similar to the one defined by [32] which can be used to quantify the distance (a.k.a. error) between a system's state and its estimation as in inequality (3.2.2).

We first define the augmented process $\begin{bmatrix}\xi & \hat{\xi}\end{bmatrix}^\top$, where ξ and $\hat{\xi}$ are the solution processes of $\mathcal{S}_S$ and $\widehat{\mathcal{S}}_S$, respectively. The corresponding augmented stochastic control system is given as

$$\mathrm{d}\begin{bmatrix}\xi\\ \hat{\xi}\end{bmatrix} = \left(\begin{bmatrix}f(\xi,u)\\ f(\hat{\xi},u)\end{bmatrix} + \begin{bmatrix}\mathbf{0}_{n\times p} & \mathbf{0}_{n\times p}\\ K & -K\end{bmatrix}\begin{bmatrix}h(\xi)\\ h(\hat{\xi})\end{bmatrix}\right)\mathrm{d}\,t + \begin{bmatrix}g_1(\xi) & \mathbf{0}_{n\times \bar{r}_2}\\ \mathbf{0}_{n\times \bar{r}_1} & Kg_2(\xi)\end{bmatrix}\begin{bmatrix}\mathrm{d}\,W_{1t}\\ \mathrm{d}\,W_{2t}\end{bmatrix}. \tag{3.4.1}$$

Next, we define a notion of stochastic solution functions which can be used to obtain the probability bound in (3.2.2).

Definition 11. *A continuous function $\phi : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ that is twice differentiable on $\mathbb{R}^n \times \mathbb{R}^n \setminus \Delta_d$ is a stochastic simulation function from $\widehat{\mathcal{S}}_S$ to $\mathcal{S}_S$ if*

1. *for all $(x,\hat{x}) \in \mathbb{R}^n \times \mathbb{R}^n$, $\phi(x,\hat{x}) \geq \varepsilon(\|x-\hat{x}\|_2)$, where ε is a $\mathcal{K}_\infty$-function;*

2. *for all $u \in \mathbb{R}^m$, $(x,\hat{x}) \in \mathbb{R}^n \times \mathbb{R}^n$ there exists a constant $\bar{c}_1 \geq 0$ and $\bar{c}_2 \geq 0$ such that $\mathcal{D}\phi(x,\hat{x},u) \leq -\bar{c}_2\phi(x,\hat{x}) + \bar{c}_1$, where the operator $\mathcal{D}$ is acting on the augmented dynamics in* (3.4.1).

The next result provides the probability bound on the estimation accuracy by using the stochastic simulation function.

Theorem 12. *Consider stochastic systems $\mathcal{S}_S$ and $\widehat{\mathcal{S}}_S$ with dynamics as in* (2.3.1) *and* (3.2.1)*, respectively, and a stochastic simulation function $\phi : \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}_{\geq 0}$ from $\widehat{\mathcal{S}}_S$ to $\mathcal{S}_S$. Then for any $\upsilon \in U$, any $\epsilon \in \mathbb{R}_{>0}$, and any $x_0, \hat{x}_0 \in \mathbb{R}^n$ the following holds:*

$$\begin{aligned}&\mathbb{P}\Big(\sup_{0\leq t\leq T}\|\xi_{x_0\upsilon}(t) - \hat{\xi}_{\hat{x}_0\upsilon}(t)\|_2 \geq \epsilon \mid x_0,\hat{x}_0\Big)\\ &\quad\leq 1 - \big(1 - \frac{\phi(x_0,\hat{x}_0)}{\varepsilon(\epsilon)}\big)e^{-\bar{c}_1 T/\varepsilon(\epsilon)}, \quad \text{if } \varepsilon(\epsilon) \geq \frac{\bar{c}_1}{\bar{c}_2},\end{aligned} \tag{3.4.2}$$

$$\begin{aligned}&\mathbb{P}\Big(\sup_{0\leq t\leq T}\|\xi_{x_0\upsilon}(t) - \hat{\xi}_{\hat{x}_0\upsilon}(t)\|_2 \geq \epsilon \mid x_0,\hat{x}_0\Big)\\ &\quad\leq \frac{\phi(x_0,\hat{x}_0) + (e^{\bar{c}_2 T} - 1)(\bar{c}_1/\bar{c}_2)}{\varepsilon(\epsilon)e^{\bar{c}_2 T}}, \quad \text{if } \varepsilon(\epsilon) \leq \frac{\bar{c}_1}{\bar{c}_2},\end{aligned} \tag{3.4.3}$$

where $T > 0$ is the time horizon.

Proof. Since ϕ is a stochastic simulation function from $\widehat{\mathcal{S}}_S$ to $\mathcal{S}_S$, one obtains the following

chain of inequality

$$\mathbb{P}\Big(\sup_{0\le t\le T}\|\xi_{x_0\upsilon}(t)-\hat{\xi}_{\hat{x}_0\upsilon}(t)\|_2\ge\epsilon\mid x_0,\hat{x}_0\Big)=\mathbb{P}\Big(\sup_{0\le t\le T}\varepsilon(\|\xi_{x_0\upsilon}(t)-\hat{\xi}_{\hat{x}_0\upsilon}(t))\|_2\ge\varepsilon(\epsilon)\mid x_0,\hat{x}_0\Big)$$
$$\le\mathbb{P}\Big(\sup_{0\le t\le T}\phi(\xi_{x_0\upsilon}(t),\hat{\xi}_{\hat{x}_0\upsilon}(t))\ge\varepsilon(\epsilon)\mid x_0,\hat{x}_0\Big)$$
$$\le\begin{cases}1-\big(1-\frac{\phi(x_0,\hat{x}_0)}{\varepsilon(\epsilon)}\big)e^{-\bar{c}_1T/\varepsilon(\epsilon)}, & \text{if } \varepsilon(\epsilon)\ge\frac{\bar{c}_1}{\bar{c}_2},\\ \frac{\phi(x_0,\hat{x}_0)+(e^{\bar{c}_2T}-1)(\bar{c}_1/\bar{c}_2)}{\varepsilon(\epsilon)e^{\bar{c}_2T}}, & \text{if } \varepsilon(\epsilon)\le\frac{\bar{c}_1}{\bar{c}_2}.\end{cases}$$

The equality holds due to the fact that ε is a $\mathcal{K}_\infty$ function. The second inequality holds based on condition 1 of Definition 11, and the last inequality follows from the result in [39, Theorem 1]. □

Next, we provide sufficient conditions under which we can construct a stochastic simulation function for linear stochastic control systems. Consider the following linear stochastic control system

$$\mathcal{S}_S:\begin{cases}\mathrm{d}\,\xi &= (A\xi+B\upsilon)\,\mathrm{d}\,t+g_1(\xi)\,\mathrm{d}\,W_{1t},\\ \mathrm{d}\,y &= C\xi\,\mathrm{d}\,t+g_2(\xi)\,\mathrm{d}\,W_{2t},\end{cases}\tag{3.4.4}$$

and the corresponding linear estimator as

$$\widehat{\mathcal{S}}_S:\mathrm{d}\,\hat{\xi}=(A\hat{\xi}+B\upsilon)\,\mathrm{d}\,t+K(\mathrm{d}\,y-C\hat{\xi}\,\mathrm{d}\,t).\tag{3.4.5}$$

Next, we impose the following assumption in order to provide the main result of this section.

Assumption 2. *Consider the linear system $\mathcal{S}_S$ in* (3.4.4)*. We assume that there exist a positive definite matrix P_ϕ, gain K, and a constant $\bar{c}_2\in\mathbb{R}_{\ge0}$ such that the following matrix inequality holds*

$$(A^\top-C^\top K^\top)P_\phi+P_\phi(A-KC)<-\bar{c}_2P_\phi.\tag{3.4.6}$$

Note that if pair (A,C) is observable, then there always exists such choices of P_ϕ and K.

From now on we assume that we are interested in studying behaviours of $\mathcal{S}_S$ over compact set $X\subset\mathbb{R}^n$. In the following lemma, we provide sufficient conditions under which one can have a quadratic stochastic simulation function from $\widehat{\mathcal{S}}_S$ to $\mathcal{S}_S$.

Lemma 13. *Consider a linear stochastic control systems $\mathcal{S}_S$ and estimator $\widehat{\mathcal{S}}_S$ as in* (3.4.4) *and* (3.4.5)*, respectively. Assume $\mathcal{S}_S$ satisfies Assumption 2 and for all $x\in X$ there exists $\bar{c}_1\ge0$ such that*

$$Tr\big(\begin{bmatrix}g_1(x) & -Kg_2(x)\end{bmatrix}^\top P_\phi\begin{bmatrix}g_1(x) & -Kg_2(x)\end{bmatrix}\big)\le\bar{c}_1.\tag{3.4.7}$$

Then

$$\phi(x,\hat{x})=(x-\hat{x})^\top P_\phi(x-\hat{x}),\tag{3.4.8}$$

is a stochastic simulation function from $\widehat{\mathcal{S}}_S$ to $\mathcal{S}_S$.

Proof. By following (3.2.3), the infinitesimal generator acting on the function ϕ is as follows:

$$\begin{aligned}\mathcal{D}\phi(x,\hat{x}) =&(x-\hat{x})^\top[(A^\top - C^\top K^\top)P_\phi + P_\phi(A-KC)](x-\hat{x})\\ &+\operatorname{Tr}\big(\begin{bmatrix}g_1(x) & -Kg_2(x)\end{bmatrix}^\top P_\phi \begin{bmatrix}g_1(x) & -Kg_2(x)\end{bmatrix}\big) \leq -\bar{c}_2\phi(x,\hat{x}) + \bar{c}_1.\end{aligned}$$

The inequality follows from (3.4.6) and (3.4.7) which implies condition 2 of Definition 11 being satisfied. Condition 1 of Definition 11 is satisfied by choosing

$$\varepsilon(s) = \frac{1}{2}\lambda_{\min}(P_\phi)s^2.$$

□

3.5 Case Study

In this section, we consider a DC motor to demonstrate the effectiveness of our results. Consider the dynamics of a DC motor given using stochastic differential equation as follows:

$$\mathcal{S}_S : \begin{cases} \mathrm{d}\begin{bmatrix}\xi_1\\ \xi_2\end{bmatrix} = \left(\overbrace{\begin{bmatrix}-\frac{R_{dc}}{L_{dc}} & -\frac{K_{dc}}{L_{dc}}\\ -\frac{K_{dc}}{J_{dc}} & -\frac{b_{dc}}{J_{dc}}\end{bmatrix}}^{A}\begin{bmatrix}\xi_1\\ \xi_2\end{bmatrix} + \begin{bmatrix}\frac{1}{L_{dc}}\\ 0\end{bmatrix}\upsilon\right)\mathrm{d}\,t + \begin{bmatrix}0.05 & 0\\ 0 & 0.05\end{bmatrix}\mathrm{d}\,W_{1t},\\ \mathrm{d}\,y = \underbrace{\begin{bmatrix}0 & 1\end{bmatrix}}_{C}\begin{bmatrix}\xi_1\\ \xi_2\end{bmatrix}\mathrm{d}\,t + 0.01\,\mathrm{d}\,W_{2t}, \end{cases} \tag{3.5.1}$$

where $\xi_1, \xi_2, \upsilon, R_{dc}, L_{dc}$ and J_{dc} are the armature current, the rotational speed of the shaft, the voltage source applied to the motor's armature, the resistance, the inductance, and the moment of inertia of the rotor, respectively. W_{1t} and W_{2t} denote the standard Brownian motions. Constant K_{dc} represents both the motor torque constant and the back emf constant. The values of the parameters are $J_{dc} = 0.01$, $b_{dc} = 0.1$, $K_{dc} = 0.01$, $R_{dc} = 1$, and $L_{dc} = 0.5$, which are adopted from [1]. From matrices A and C, one can readily see that the system is observable. We consider the state set $X = \begin{bmatrix}-0.1 & 0.1\end{bmatrix} \times \begin{bmatrix}-0.5 & 0.5\end{bmatrix}$, and regions of interest $X_0 = \begin{bmatrix}-0.01 & 0.01\end{bmatrix} \times \begin{bmatrix}-0.2 & 0.2\end{bmatrix}$, $X_1 = \begin{bmatrix}-0.1 & -0.05\end{bmatrix} \times \begin{bmatrix}-0.5 & -0.3\end{bmatrix} \cup \begin{bmatrix}0.05 & 0.1\end{bmatrix} \times \begin{bmatrix}0.3 & 0.5\end{bmatrix}$. The aim is to compute a controller with a potentially tight upper bound on the probability of the states starting from the initial set X_0 reaching the unsafe set X_1 within time horizon $T = 10$, as in (3.3.5). We compute matrices

$$K = \begin{bmatrix}0.0069\\ 0.0027\end{bmatrix}, P_\phi = \begin{bmatrix}0.0554 & 0.0053\\ 0.0053 & 0.3209\end{bmatrix},$$

and $\bar{c}_2 = 0.1$ satisfying (3.4.6) by converting it to an LMI using Schur complement. The stochastic simulation function according to Lemma 13 is given as $\phi(x,\hat{x}) = (x-\hat{x})^\top P_\phi(x-\hat{x})$

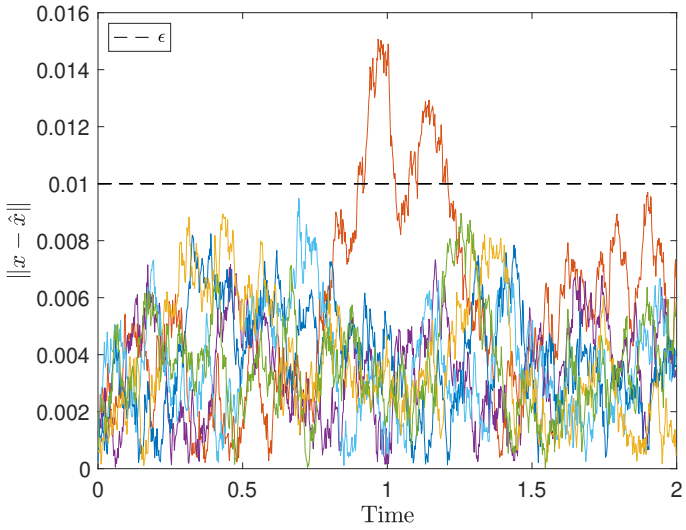

Figure 3.1: A few realizations of the errors between concrete state trajectories and estimated trajectories.

with $\varepsilon(s) = 0.02768s^2$ and $\bar{c}_1 = 3.7693 \times 10^{-7}$. By use of the results in Theorem 12 we obtain $\theta = 0.1272$ by choosing $\epsilon = 0.01$. The obtained probability that is at least 87.28% is also empirically verified by computing distance between trajectories of the concrete system and the estimated system at time using 10000 realizations. Several realizations are shown in Figure 3.1.

A quadratic control barrier function using the approach discussed in Subsection 3.3.1 is obtained as follows:

$$\mathcal{B}(\hat{x}) = 290.9438\hat{x}_1^2 + 10.98940\hat{x}_1\hat{x}_2 + 1.1977\hat{x}_2^2,$$

and the corresponding controller as

$$\mathsf{u}(\hat{x}) = 0.2721\hat{x}_1 + 1.3607\hat{x}_2. \tag{3.5.2}$$

with the values $\beta_0 = 0.099$, $\bar{c}_1 = 1 \times 10^{-5}$, $T = 10$. All the computations are done using GUROBI and YALMIP [40]. The lower bound in (3.3.6) is computed as:

$$\mathbb{P}\Big\{\forall t \in [0, T), \xi_{x_0 v}(t) \notin X_1\Big\} \geq 0.8647, \ \forall x_0 \in X_0.$$

Figure 3.2 shows a few realizations of the trajectories starting from the initial region X_0 under the controller (3.5.2).

3.6 Summary

In this chapter, we provided a framework for designing control barrier functions for partially-observable stochastic control systems subjected to noisy measurements. The controllers associated with control barrier functions provide the upper bound on the probability

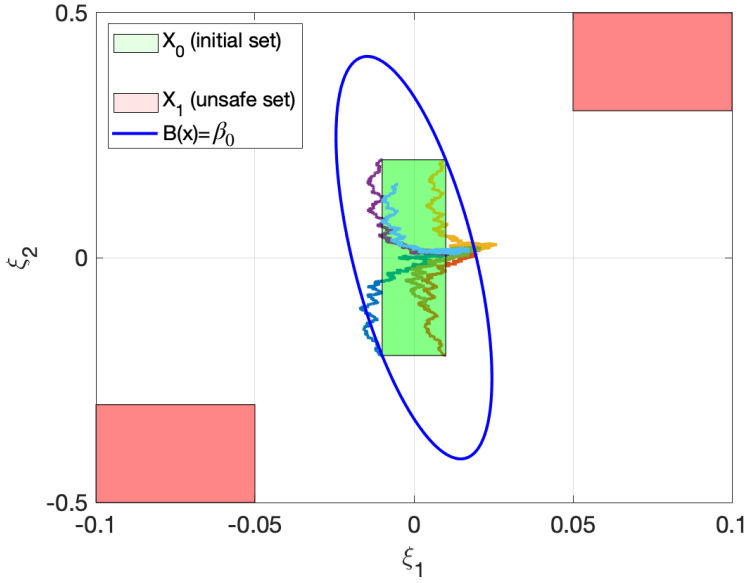

Figure 3.2: A few realizations of the closed-loop trajectories using controller (3.5.2). The blue ellipsoid shows the β_0-level set of $\mathcal{B}$, defined as $\{\hat{x} \in X \mid \mathcal{B}(\hat{x}) = \beta_0\}$.

that the system reaches an unsafe region in a finite time horizon. This upper bound is provided by utilizing the probability bound obtained for the accuracy of the estimator via the notion of stochastic simulation functions.

243. Controller Synthesis for Partially-Observable Stochastic Control Systems

Chapter 4

Synthesis of Partially-Observable Jump-Diffusion Systems

In this chapter, we study formal synthesis of controllers for partially-observable jump-diffusion systems against complex logic specifications. Given a state estimator, we utilize a discretization-free approach for formal synthesis of control policies by using a notation of control barrier functions without requiring any knowledge of the estimation accuracy. Our goal is to synthesize an offline control policy providing (potentially maximizing) a lower bound on the probability that the trajectories of the partially-observable jump-diffusion system satisfy some complex specifications expressed by deterministic finite automata.

4.1 Introduction

Recent years have witnessed a growing interest in formal synthesis of controllers for complex systems against complex logic specifications [7]. These specifications are usually expressed using temporal logic formulae or as (in)finite strings over finite automata. In general, the problem is very challenging, and a closed-form solution does not exist. In this regard, approximate or probabilistic solutions have been used to synthesize controllers enforcing complex logic specifications for stochastic control systems.

4.1.1 Related Literature

Several approaches based on finite abstractions have been widely used to formally synthesize policies enforcing complex logic specifications. Existing techniques include policy synthesis enforcing linear temporal logic specifications for non-stochastic systems [6, 41] and for stochastic ones [42, 43, 44]. In these approaches, which rely on the discretization of the state set, an abstract system is used as a substitution for the original system. Moreover, a (probabilistic) error between the original systems and that of their finite abstractions is also computed.

To alleviate the curse of dimensionality appearing in large systems, control barrier functions are used in order to solve the formal synthesis problem against complex specifications. To this end, barrier functions were used in [45] to verify temporal properties in nonlinear deterministic systems. As an extension of [45], the results in [46] verify hybrid dynamical systems against syntactically co-safe linear temporal logic (LTL) specifications using barrier functions. The results in [47] utilizes time-varying control barrier functions for control synthesis under signal temporal logic tasks. The results in [48] and [49] use barrier functions for the formal verification of hyperproperties (properties that are described over sets of traces) in control systems. As for stochastic systems, the results in [50] use barrier functions to verify discrete-time stochastic systems against safe LTL over finite traces, and provide a lower bound on the probability of satisfaction. The proposed approach in [51] provides sufficient conditions on probabilistic reach-avoid-stay specification using stochastic Lyapunov-barrier functions. By utilizing control barrier functions and composing risk metrics with stochastic predicates, the authors in [52] provide risk signal temporal logic (RiSTL) to quantify the risk by which a predicate is not satisfied in a stochastic control system.

Note that the aforementioned works assume the availability of complete state information, while in many real applications we do not have access to complete state information. To this end, the results in [53] provide an approach to synthesize controllers for POMDPs with LTL specifications such that the probability of satisfying LTL formulae is maximized. In Chapter 3, we considered the problem of synthesizing controllers for partially-observable stochastic control systems. In particular, we searched for a control barrier function that provides a controller along with a lower bound on the probability that the system satisfies invariance specifications over a finite-time horizon. This chapter is an extension of the previous chapter to solve the problem of controller synthesis for partially-observable jump-diffusion systems against complex temporal logic specifications. The approach provided in this chapter does not require prior knowledge of the estimation accuracy, which is a requirement in the results proposed in Chapter 3.

4.1.2 Contribution

The contents of this chapter have been published in the IEEE Control Systems Letters [55]. It is a joint work with Prof. Pushpak Jagtap and Prof. Majid Zamani. The author of the thesis has established the results and written the draft. Pushpak Jagtap contributed to the initial discussions, the results, the revision of the draft, and mentoring. Majid Zamani supervised the work.

The contributions of this chapter are twofold. First, we provide a controller synthesis approach enforcing complex logic specifications expressed by (non)deterministic finite automata for partially-observable jump-diffusion systems. As a special case, those properties include invariance ones. Second, we provide an approach for computing a lower bound on the probability that the system satisfies given specifications over a finite-time horizon *without* requiring any knowledge of the estimator's accuracy.

4.2 Preliminaries and Problem Definition

For the PO-JDS $\mathcal{S}_J$ in (2.3.2), we first raise the following assumption on the existence of the estimator that estimates the state of S_J.

Assumption 3. *The states of the PO-JDS $\mathcal{S}_J$ in (2.3.2) can be estimated by a proper estimator $\widehat{\mathcal{S}}_J$ represented in the form of an SDE as:*

$$\widehat{\mathcal{S}}_J : \mathrm{d}\,\hat{\xi} = f(\hat{\xi}, \upsilon)\,\mathrm{d}\,t + K\big(\mathrm{d}\,y - h(\hat{\xi})\,\mathrm{d}\,t\big), \tag{4.2.1}$$

where $K \in \mathbb{R}^{n\times p}$ is the estimator gain.

There are plenty of results in the literature on the computation of estimator gain K for various classes of stochastic systems; see the results in [16, 56, 57], and [58]. We define the augmented process $[\xi, \hat{\xi}]^\top$, where ξ and $\hat{\xi}$ are the solution processes of $\mathcal{S}_J$ and $\widehat{\mathcal{S}}_J$, respectively. The corresponding augmented jump-diffusion system $\widetilde{\mathcal{S}}_J$ can be defined as:

$$\begin{aligned}\begin{bmatrix}\mathrm{d}\,\xi\\ \mathrm{d}\,\hat{\xi}\end{bmatrix} =& \Big(\begin{bmatrix}f(\xi,\upsilon)\\ f(\hat{\xi},\upsilon)\end{bmatrix} + \begin{bmatrix}\mathbf{0}_{n\times p} & \mathbf{0}_{n\times p}\\ K & -K\end{bmatrix}\begin{bmatrix}h(\xi)\\ h(\hat{\xi})\end{bmatrix}\Big)\,\mathrm{d}\,t\\ &+\begin{bmatrix}g_1(\xi) & \mathbf{0}_{n\times\bar{r}_2}\\ \mathbf{0}_{n\times\bar{r}_1} & Kg_2(\xi)\end{bmatrix}\begin{bmatrix}\mathrm{d}\,W_{1t}\\ \mathrm{d}\,W_{2t}\end{bmatrix}+\begin{bmatrix}r_1(\xi)\\ \mathbf{0}_{n\times\bar{q}_1}\end{bmatrix}\mathrm{d}\,P_{1t}+\begin{bmatrix}\mathbf{0}_{n\times\bar{q}_2}\\ Kr_2(\xi)\end{bmatrix}\mathrm{d}\,P_{2t}.\end{aligned} \tag{4.2.2}$$

For later use, we provide the definition of the infinitesimal generator for $\widetilde{\mathcal{S}}_J$ using Ito's differentiation [20]. Let $\mathcal{B} : X\times X \to \mathbb{R}$ be a twice differentiable function. The infinitesimal generator of $\mathcal{B}$ associated with the system $\widetilde{\mathcal{S}}_J$ for all $(x,\hat{x}) \in X \times X$ and for all $u \in U$ is given by

$$\begin{aligned}\mathcal{D}\mathcal{B}(x,\hat{x},u) =& \begin{bmatrix}\partial_x\mathcal{B} & \partial_{\hat{x}}\mathcal{B}\end{bmatrix}\Big(\begin{bmatrix}f(x,u)\\ f(\hat{x},u)\end{bmatrix} + \begin{bmatrix}\mathbf{0}_{n\times p} & \mathbf{0}_{n\times p}\\ K & -K\end{bmatrix}\begin{bmatrix}h(x)\\ h(\hat{x})\end{bmatrix}\Big)\\ &+\frac{1}{2}\mathrm{Tr}\Big(\begin{bmatrix}g_1(x) & 0_{n\times\bar{r}_2}\\ \mathbf{0}_{n\times\bar{r}_1} & Kg_2(x)\end{bmatrix}\begin{bmatrix}g_1(x) & 0_{n\times\bar{r}_2}\\ \mathbf{0}_{n\times\bar{r}_1} & Kg_2(x)\end{bmatrix}^\top\begin{bmatrix}\partial_{xx}\mathcal{B} & \partial_{x\hat{x}}\mathcal{B}\\ \partial_{\hat{x}x}\mathcal{B} & \partial_{\hat{x}\hat{x}}\mathcal{B}\end{bmatrix}\Big)\\ &+\sum_{i=1}^{\bar{q}_1}\lambda_{1i}(\mathcal{B}(x+r_1(x)\mathrm{e}_i,\hat{x})-\mathcal{B}(x,\hat{x})) + \sum_{i=1}^{\bar{q}_2}\lambda_{2i}(\mathcal{B}(x+Kr_2(x)\mathrm{e}_i,\hat{x})-\mathcal{B}(x,\hat{x})).\end{aligned} \tag{4.2.3}$$

The symbols ∂_x and $\partial_{x,\hat{x}}$ in (4.2.3) represent first and second-order partial derivatives with respect to x (1st argument) and $\hat{x}$ (2nd argument), respectively. Note that we dropped the arguments of $\partial_x\mathcal{B}$, $\partial_{\hat{x}}\mathcal{B}$, $\partial_{x,x}\mathcal{B}$, $\partial_{x,\hat{x}}\mathcal{B}$, $\partial_{\hat{x},x}\mathcal{B}$, and $\partial_{\hat{x},\hat{x}}\mathcal{B}$ in (4.2.3) for the sake of simplicity.

Given a PO-JDS $\mathcal{S}_J$ in (2.3.2), we aim at synthesizing a control policy that guarantees a potentially tight lower bound on the probability that system $\mathcal{S}_J$ satisfies a complex specification over a finite time horizon. The class of specifications considered in this chapter are provided in the next subsection.

Remark 14. *The use of the augmented system $\widetilde{\mathcal{S}}_J$ will allow us to provide the main result of this chapter without any correctness requirement on the observer. In particular, our augmented system formulation provides the user the flexibility to design any observer by means of any technique. The probabilistic distance between the values of state and their estimator is natively considered in our formulation and one does not need to quantify this distance a-priori which is needed in the results proposed in [16, 54].*

4.2.1 Specifications

In this subsection, we consider the class of specifications expressed by nondeterministic finite automata (NFA) as defined below.

Definition 15. *[4] A nondeterministic finite automaton (NFA) is a tuple $\mathcal{A} = (Q, Q_0, \Sigma, \delta, F)$, where Q is a finite set of states, $Q_0 \subseteq Q$ is a set of initial states, Σ is a finite set (a.k.a. alphabet), $\delta : Q \times \Sigma \to P(Q)$ is a transition function, where $P(Q)$ denotes the power set of Q, and $F \subseteq Q$ is a set of accepting (or final) states.*

NFA $\mathcal{A}$ is called *deterministic* if the transition function is defined as $\delta : Q \times \Sigma \to Q$, and we refer to it as deterministic finite automata (DFA). Since every NFA can be converted to its equivalent DFA using the powerset construction [59], in the rest of this chapter, we only deal with DFA. Moreover, it is well known that the complement of a DFA $\mathcal{A}$, denoted by $\mathcal{A}^c$, is again a DFA [60]. We use the notation $q \xrightarrow{\varpi} q'$ to denote transition relation $(q, \varpi, q') \in \delta$. A finite word $\varpi = (\varpi_0, \varpi_1, \ldots, \varpi_{k-1}) \in \Sigma^k$ is accepted by DFA $\mathcal{A}$ if there exists a finite state run $\mathbf{q} = (q_0, q_1, \ldots, q_k) \in Q^{k+1}$ such that $q_0 \in Q_0$, $q_i \xrightarrow{\varpi_i} q_{i+1}$ for all $0 \leq i < k$ and $q_k \in F$. The accepted language of $\mathcal{A}$, denoted by $\mathcal{L}(\mathcal{A})$, is the set of all words accepted by $\mathcal{A}$.

In this chapter, we consider those specifications given by the accepting languages of DFA $\mathcal{A}$ defined over a set of atomic propositions Π, *i.e.*, the alphabet $\Sigma = \Pi$. We should highlight that all linear temporal logic specifications defined over finite traces, referred to as LTL_F, are recognized by DFA [61].

4.2.2 Satisfaction of Specification by PO-JDS

A given PO-JDS $\mathcal{S}_J$ in (2.3.2) is connected to the specification given by the accepting language of a DFA $\mathcal{A}$ defined over a set of atomic propositions Π, with the help of a measurable labeling function $L : X \to \Pi$ as described in the next definition which is similar to [45, Definition 2].

Definition 16. *For a PO-JDS $\mathcal{S}_J$ as in (2.3.2) and the labeling function $L : X \to \Pi$, a finite sequence $\varpi(\xi_{x_0 \upsilon}) = (\varpi_0, \varpi_1, \ldots, \varpi_{k-1}) \in \Pi^k$, $k \in \mathbb{N}$, is a finite trace of the solution process $\xi_{x_0 \upsilon}$ over a finite time horizon $[0, T) \subset \mathbb{R}_{\geq 0}$ if there exists an associated time sequence $t_0, t_1, \ldots, t_{k-1}$ such that $t_0 = 0$, $t_k = T$, and for all $j \in \{0, 1, \ldots, k-1\}$, $t_j \in \mathbb{R}_{\geq 0}$ following conditions hold*

- $t_j < t_{j+1}$;

- $\xi_{x_0\upsilon}(t_j) \in L^{-1}(\varpi_j)$;

- *If* $\varpi_j \neq \varpi_{j+1}$, *then for some* $t'_j \in [t_j, t_{j+1}]$, $\xi_{x_0\upsilon}(t) \in L^{-1}(\varpi_j)$ *for all* $t \in (t_j, t'_j)$; $\xi_{x_0\upsilon}(t) \in L^{-1}(\varpi_{j+1})$ *for all* $t \in (t'_j, t_{j+1})$; *and either* $\xi_{x_0\upsilon}(t'_j) \in L^{-1}(\varpi_j)$ *or* $\xi_{x_0\upsilon}(t'_j) \in L^{-1}(\varpi_{j+1})$.

Next, we define the probability that the solution process $\xi_{x_0\upsilon}$ of the PO-JDS $\mathcal{S}_J$ starting from some initial state $\xi_{x_0\upsilon}(0) = x_0 \in X_0$ under control policy υ satisfies the specification given by DFA $\mathcal{A}$.

Definition 17. *The finite trace corresponding to the solution process of a PO-JDS* $\mathcal{S}_J$ *in* (2.3.2) *starting from* $x_0 \in X_0$ *and under the control policy* υ *over a finite-time horizon* $[0, T) \subset \mathbb{R}_{\geq 0}$, *i.e.,* $\varpi(\xi_{x_0\upsilon}) = (\varpi_0, \varpi_1, \ldots, \varpi_j, \ldots, \varpi_{k-1}) \in \Pi^k$ *as in Definition 16, satisfies a specification given by the language of a DFA* $\mathcal{A}$, *denoted by* $\varpi(\xi_{x_0\upsilon}) \models \mathcal{A}$, *if there exists* $j \in \{0, \ldots, k-1\}$ *such that* $(\varpi_0, \varpi_1, \ldots, \varpi_j) \in \mathcal{L}(\mathcal{A})$. *The probability of satisfaction of the specification given by* $\mathcal{A}$ *is denoted by* $\mathbb{P}\{\varpi(\xi_{x_0\upsilon}) \models \mathcal{A}\}$.

Remark 18. *The set of atomic propositions* $\Pi = \{p_0, p_1, \ldots, p_M\}$ *and the labeling function* $L : X \to \Pi$ *provide a measurable partition of the state set* $X = \cup_{i=1}^{N} X_i$ *as* $X_i := L^{-1}(p_i)$. *Without loss of generality, we assume that* $X_i \neq \emptyset$ *for any* i.

4.2.3 Problem Definition

Now, we formally define the main synthesis problem considered in this chapter.

Problem 19. *Given a PO-JDS* $\mathcal{S}_J$ *as in* (2.3.2), *a specification given by the accepting language of DFA* $\mathcal{A} = (Q, Q_0, \Pi, \delta, F)$ *over a set of atomic propositions* $\Pi = \{p_0, p_1, \ldots, p_M\}$, *a labeling function* $L : X \to \Pi$, *and a real value* $\vartheta \in (0, 1)$, *compute an offline control policy* υ *(if existing) such that* $\mathbb{P}\{\varpi(\xi_{x_0\upsilon}) \models \mathcal{A}\} \geq \vartheta$, *for all* $x_0 \in L^{-1}(p_i)$ *and some* $i \in \{0, 1, \ldots, M\}$.

Finding a solution to Problem 19 (if existing) is difficult in general. Our approach is to compute a policy υ together with a lower bound $\underline{\vartheta}$. Our aim is to find the potentially largest lower bound, which can be compared with ϑ and gives policy, i.e., a solution for Problem 19 if $\underline{\vartheta} \geq \vartheta$. Instead of computing a control policy that guarantees the lower bound $\underline{\vartheta}$, we compute a policy that guarantees $\mathbb{P}\{\varpi(\xi_{x_0\upsilon}) \models \mathcal{A}^c\} \leq \bar{\vartheta}$, for any $x_0 \in L^{-1}(p_i)$ and some $i \in \{0, 1, \ldots, M\}$. Then for the same control policy the lower bound can be easily obtained as $\underline{\vartheta} = 1 - \bar{\vartheta}$. This is done by constructing a DFA $\mathcal{A}^c$ whose language is the complement of the language of DFA $\mathcal{A}$. To synthesize a controller, we utilize the notion of control barrier functions defined for augmented jump-diffusion system $\widetilde{\mathcal{S}}_J$ introduced in the next section.

4.3 Control Barrier Functions for PO-JDSs

In this section, we provide sufficient conditions using so-called control barrier functions under which we can provide the upper bound on the probability that the trajectories of system $\mathcal{S}_J$ starting from any initial state in $X_0 \subseteq X$ reach $X_1 \subseteq X$. To provide a result giving an upper bound on the reachability probability for the trajectory of $\mathcal{S}_J$, we provide conditions on barrier functions constructed over the augmented system $\widetilde{\mathcal{S}}_J$.

Theorem 20. *Consider a PO-JDS $\mathcal{S}_J$ as in (2.3.2), its estimator $\widehat{\mathcal{S}}_J$ as in (4.2.1), the resulting augmented system $\widetilde{\mathcal{S}}_J$ as in (4.2.2) and sets $X_0, X_1 \subseteq X$. Suppose there exists a twice differentiable function $\mathcal{B} : X \times X \to \mathbb{R}_{\geq 0}$, constants $c \geq 0$ and $\beta_0 \in [0, 1)$ such that*

$$\forall (x, \hat{x}) \in X_0 \times X_0, \qquad \mathcal{B}(x, \hat{x}) \leq \beta_0, \tag{4.3.1}$$
$$\forall (x, \hat{x}) \in X_1 \times X, \qquad \mathcal{B}(x, \hat{x}) \geq 1, \tag{4.3.2}$$
$$\forall \hat{x} \in X, \exists u \in U, \forall x \in X, \quad \mathcal{D}\mathcal{B}(x, \hat{x}, u) \leq c. \tag{4.3.3}$$

Then, the probability that the solution process $\xi_{x_0\upsilon}$ of the system $\mathcal{S}_J$ starts from any initial state $x_0 \in X_0$ and reaches region X_1 under the control policy υ within time horizon $[0, T) \subset \mathbb{R}_{\geq 0}$ is upper bounded by $\beta_0 + cT$.

Proof. By using (4.3.1) and the fact that $X_1 \times X \subseteq \big\{(x, \hat{x}) \in X \times X \mid \mathcal{B}(x, \hat{x}) \geq 1\big\}$, we have $\mathbb{P}\big\{\xi_{x_0\upsilon}(t) \in X_1 \wedge \hat{\xi}_{\hat{x}_0\upsilon}(t) \in X \ \exists t \in [0, T) \mid x_0, \hat{x}_0\big\} \leq \mathbb{P}\big\{\sup_{0\leq t\leq T}\mathcal{B}(\xi_{x_0\upsilon}(t), \hat{\xi}_{\hat{x}_0\upsilon}(t)) \geq 1 \mid x_0, \hat{x}_0\big\} \leq \mathcal{B}(x_0, \hat{x}_0) + cT \leq \beta_0 + cT$. The second inequality is obtained by utilizing the result of [33, Theorem 1]. This implies that the probability of the augmented trajectory of $\widetilde{\mathcal{S}}_J$ staring from any $(x_0, \hat{x}_0) \in X_0 \times X_0$ and reaching $X_1 \times X$ is upper bounded by $\beta_0 + cT$. Now we get $\mathbb{P}\big\{\xi_{x_0\upsilon}(t) \in X_1 \wedge \hat{\xi}_{\hat{x}_0\upsilon}(t) \in X \ \exists t \in [0, T) \mid x_0, \hat{x}_0\big\} \leq \mathbb{P}\big\{\xi_{x_0\upsilon}(t) \in X_1 \ \exists t \in [0, T) \mid x_0\big\} + \mathbb{P}\big\{\hat{\xi}_{\hat{x}_0\upsilon}(t) \in X \ \exists t \in [0, T) \mid \hat{x}_0\big\} - \mathbb{P}\big\{\xi_{x_0\upsilon}(t) \in X_1 \vee \hat{\xi}_{\hat{x}_0\upsilon}(t) \in X \ \exists t \in [0, T) \mid x_0, \hat{x}_0\big\}$. Since the second and last terms trivially hold with probability 1, one has $\mathbb{P}\big\{\xi_{x_0\upsilon}(t) \in X_1 \wedge \hat{\xi}_{\hat{x}_0\upsilon}(t) \in X \ \exists t \in [0, T) \mid x_0, \hat{x}_0\big\} \leq \mathbb{P}\big\{\xi_{x_0\upsilon}(t) \in X_1 \ \exists t \in [0, T) \mid x_0\big\}$. Now, since the right term of the `and` (*i.e.*, $\wedge$) is held for all time, the inequality above becomes an equality and one gets $\mathbb{P}\big\{\xi_{x_0\upsilon}(t) \in X_1 \ \exists t \in [0, T) \mid x_0\big\} \leq \beta_0 + Tc$ which concludes the proof. □

The function $\mathcal{B}$ in Theorem 20 satisfying (4.3.1)-(4.3.3) is usually referred to as the control barrier function for $\widehat{\mathcal{S}}_J$.

Remark 21. *Condition (4.3.3) implicitly associates a stationary controller $\mathsf{u} : X \to U$ according to the existential quantifier on u for any $\hat{x} \in X$ and is independent of choice of $x \in X$. The stationary control policy υ driving the system is readily given by $\upsilon(t) = \mathsf{u}(\hat{\xi}_{x_0\upsilon}(t))$, where $\hat{\xi}_{x_0\upsilon}$ is the solution process of the estimator.*

4.4 Formal Synthesis of Controllers

To synthesize control policies using control barrier functions enforcing specifications expressed by DFA $\mathcal{A}$, we first provide the decomposition of specifications into sequential reachability tasks which will later be solved using control barrier functions.

4.4.1 Decomposition into Sequential Reachability

Consider a DFA $\mathcal{A}$ expressing the properties of interest for the system $\mathcal{S}_J$. Consider DFA $\mathcal{A}^c = (Q, Q_0, \Pi, \delta, F)$ whose language is the complement of the language of DFA $\mathcal{A}$. The sequence $\mathbf{q} = (q_0, q_1, \ldots, q_k) \in Q^{k+1}$, $k \in \mathbb{N}$ is called an accepting state run if $q_0 \in Q_0$, $q_k \in F$, and there exists a finite word $\varpi = (\varpi_0, \varpi_1, \ldots, \varpi_{k-1}) \in \Pi^k$ such that $q_i \xrightarrow{\varpi_i} q_{i+1}$ for all $i \in \{0, 1, \ldots, k-1\}$. We denote the finite word corresponding to accepting state run $\mathbf{q}$ by $\varpi(\mathbf{q})$. We also indicate the length of $\mathbf{q} \in Q^{k+1}$ by $|\mathbf{q}|$, which is $k+1$. Let $\mathcal{R}$ be the set of all finite accepting state runs starting from $q_0 \in Q_0$ excluding self-loops, where

$$\mathcal{R} := \{\mathbf{q} = (q_0, q_1, \ldots, q_k) \in Q^{k+1} \mid q_k \in F, q_i \neq q_{i+1}, \forall i < k\}.$$

Computation of $\mathcal{R}$ can be done algorithmically by viewing $\mathcal{A}^c$ as a directed graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$ with vertices $\mathcal{V} = Q$ and edges $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ such that $(q, q') \in \mathcal{E}$ if and only if $q' \neq q$ and there exist $p \in \Pi$ such that $q \xrightarrow{p} q'$. For any $(q, q') \in \mathcal{E}$, we donate the atomic proposition associated with the edge (q, q') by $\varpi(q, q')$. From the construction of the graph, it is obvious that the finite path in the graph starting from vertices $q_0 \in Q_0$ and ending at $q_F \in F$ is an accepting state run $\mathbf{q}$ of $\mathcal{A}^c$ without any self-loop and therefore belongs to $\mathcal{R}$. One can easily compute $\mathcal{R}$ using depth first search algorithm [62]. For each $p \in \Pi$, we define a set $\mathcal{R}^p$ as

$$\mathcal{R}^p := \{\mathbf{q} = (q_0, q_1, \ldots, q_k) \in \mathcal{R} \mid \varpi(q_0, q_1) = p\}. \tag{4.4.1}$$

Decomposition into sequential reachability is performed as follows. For any $\mathbf{q} = (q_0, q_1, \ldots, q_k) \in \mathcal{R}^p$ $\forall p \in \Pi$, we define $\mathcal{P}^p(\mathbf{q})$ as a set of all state runs of length 3,

$$\mathcal{P}^p(\mathbf{q}) := \{(q_i, q_{i+1}, q_{i+2}) \mid 0 \leq i \leq k-2\}. \tag{4.4.2}$$

Now, we define $\mathcal{P}(\mathcal{A}^c) := \bigcup_{p \in \Pi} \bigcup_{\mathbf{q} \in \mathcal{R}^p} \mathcal{P}^p(\mathbf{q})$.

Remark 22. *Note that $\mathcal{P}^p(\mathbf{q}) = \emptyset$ for $|\mathbf{q}| = 2$. In fact, any accepting state run of length 2 specifies a subset of the state set such that the system satisfies $\mathcal{A}^c$ whenever it starts from that subset. This gives trivial zero probability for satisfying the specification, thus neglected in the sequel.*

For the illustration of the above sets, we kindly refer the interested reader to Example 1 in [13]. Having $\mathcal{P}^p(\mathbf{q})$ in (4.4.2) as the set of state runs of length 3, in this subsection, we provide a systematic approach to compute a policy together with a (potentially tight) lower bound on the probability that the solution process of $\mathcal{S}_J$ satisfies the specifications given by

DFA $\mathcal{A}$. Given a DFA $\mathcal{A}^c$, our approach relies on performing a reachability computation over each element of $\mathcal{P}(\mathcal{A}^c)$ (*i.e.*, $\bigcup_{p\in\Pi}\bigcup_{\mathbf{q}\in\mathcal{R}^p}\mathcal{P}^p(\mathbf{q})$), where reachability probability is upper bounded using control barrier functions along with appropriate choices of control inputs as mentioned in Theorem 20. However, computation of control barrier functions and the policies for each element $\nu \in \mathcal{P}(\mathcal{A}^c)$, can cause ambiguity while utilizing controllers in closed-loop whenever there are more than one outgoing edges from a state of the automaton. To resolve this ambiguity, we simply merge such reachability problems into one reachability problem by replacing the reachable set $X_1 \times X$ in Theorem 20 with the union of regions corresponding to the alphabets of all outgoing edges. Thus we get a common control barrier function and a corresponding controller. This enables us to partition $\mathcal{P}(\mathcal{A}^c)$ and put the elements sharing a common control barrier function and a corresponding controller in the same partition set. These sets can be formally defined as

$$\mu_{(q,q',\Delta(q'))} := \{(q,q',q'') \in \mathcal{P}(\mathcal{A}^c) \mid q,q',q'' \in Q \text{ and } q'' \in \Delta(q')\}.$$

The control barrier function and the controller (as discussed in Remark 21) corresponding to the partition set $\mu_{(q,q',\Delta(q'))}$ are denoted by $\mathcal{B}_{\mu_{(q,q',\Delta(q'))}}(x,\hat{x})$ and $\mathsf{u}_{\mu_{(q,q',\Delta(q'))}}(\hat{x})$, respectively. Thus, for all $\nu \in \mathcal{P}(\mathcal{A}^c)$, we have

$$\mathcal{B}_\nu(x,\hat{x}) = \mathcal{B}_{\mu_{(q,q',\Delta(q'))}}(x,\hat{x}) \text{ and } \mathsf{u}_\nu(\hat{x}) = \mathsf{u}_{\mu_{(q,q',\Delta(q'))}}(\hat{x}), \text{if } \nu \in \mu_{(q,q',\Delta(q'))}. \tag{4.4.3}$$

4.4.2 Control Policy

From the above discussion, one can readily observe that we have different control policies at different locations of the automaton which can be interpreted as a switching control policy. Next, we define the automaton representing the switching mechanism for control policies. Consider the DFA $\mathcal{A}^c = (Q, Q_0, \Pi, \delta, F)$ corresponding to the complement of DFA $\mathcal{A}$ as discussed in Section 4.4.1, where $\Delta(q)$ denotes the set of all successor states of $q \in Q$. Now, the switching mechanism is given by a DFA $\mathcal{A}_\mathfrak{m} = (Q_\mathfrak{m}, Q_{\mathfrak{m}0}, \Pi_\mathfrak{m}, \delta_\mathfrak{m}, F_\mathfrak{m})$, where $Q_\mathfrak{m} := Q_{\mathfrak{m}0} \cup \{(q,q',\Delta(q')) \mid q,q' \in Q \setminus F\} \cup F_\mathfrak{m}$ is the set of states, $Q_{\mathfrak{m}0} := \{(q_0,\Delta(q_0)) \mid q_0 \in Q_0\}$ is the set of initial states, $\Pi_\mathfrak{m} = \Pi$, $F_\mathfrak{m} = F$, and the transition relation $(q_\mathfrak{m}, \varpi, q'_\mathfrak{m}) \in \delta_\mathfrak{m}$ is defined as

- for all $q_\mathfrak{m} = (q_0,\Delta(q_0)) \in Q_{\mathfrak{m}0}$, $(q_0,\Delta(q_0)) \xrightarrow{\varpi(q_0,q'')} (q_0,q'',\Delta(q''))$, where $q_0 \xrightarrow{\varpi(q_0,q'')} q''$;
- for all $q_\mathfrak{m} = (q,q',\Delta(q')) \in Q_\mathfrak{m} \setminus (Q_{\mathfrak{m}0} \cup F_\mathfrak{m})$,
  - $(q,q',\Delta(q')) \xrightarrow{\varpi(q',q'')} (q',q'',\Delta(q''))$, such that $q,q',q'' \in Q$, $q' \xrightarrow{\varpi(q',q'')} q''$, and $q'' \notin F$; and
  - $(q,q',\Delta(q')) \xrightarrow{\varpi(q',q'')} q''$, such that $q,q',q'' \in Q$, $q' \xrightarrow{\varpi(q',q'')} q''$, and $q'' \in F$.

The hybrid controller defined over augmented state-space $X \times Q_{\mathsf{m}}$ that is a candidate for solving Problem 19 is given by

$$\tilde{\mathsf{u}}(\hat{x}, q_{\mathsf{m}}) = \mathsf{u}_{\mu_{(q'_{\mathsf{m}})}}(\hat{x}), \quad \forall (q_{\mathsf{m}}, L(\hat{x}), q'_{\mathsf{m}}) \in \delta_{\mathsf{m}}. \tag{4.4.4}$$

The corresponding hybrid control policy υ is given by $\upsilon(t) = \tilde{\mathsf{u}}(\hat{\xi}(t), q_{\mathsf{m}})$. For the illustration of the switching mechanism, see Example 1 in [13, Section 5]. In the next subsection, we discuss the computation of bound on the probability of satisfying the specification under such a policy, which then can be used for checking if this policy is indeed a solution for Problem 19.

4.4.3 Computation of Probability

The next theorem provides an upper bound on the probability that the solution process satisfies the specifications given by $\mathcal{A}$.

Theorem 23. *For a specification given by the accepting language of DFA $\mathcal{A}$, let $\mathcal{A}^c$ be the DFA corresponding to the complement of $\mathcal{A}$, $\mathcal{R}^p$ be the set defined in* (4.4.1)*, and $\mathcal{P}^p$ be the set of runs of length* 3 *defined in* (4.4.2)*. Then the probability that the solution process of the system $\mathcal{S}_J$ starting from any initial state $x_0 \in L^{-1}(p)$ under the hybrid control policy υ associated with the hybrid controller* (4.4.4) *satisfies $\mathcal{A}^c$ within time horizon $[0, T)$ is upper bounded by*

$$\mathbb{P}\{\varpi(\xi_{x_0\upsilon}) \models \mathcal{A}^c\} \leq \sum_{\mathbf{q} \in \mathcal{R}^{\mathbf{p}}} \prod \{(\beta_{0\nu} + c_\nu T) \,|\, \nu = (q, q', q'') \in \mathcal{P}^p(\mathbf{q})\}, \tag{4.4.5}$$

where $\beta_{0\nu} + c_\nu T$ is the upper bound on the probability that the solution process of $\mathcal{S}_J$ starts from $X_0 := L^{-1}(\varpi(q, q'))$ and reaches $X_1 := L^{-1}(\varpi(q', q''))$ under control policy υ within time horizon $[0, T)$ which is computed via Theorem 20.

Proof. The proof is similar to that of [13, Theorem 5.2] and is therefore omitted. □

Theorem 23 enables us to decompose the specification into a collection of sequential reachabilities, compute bounds on the reachability probabilities using Theorem 20, and then combine the bounds in a sum-product expression.

Remark 24. *In case we are unable to find control barrier functions for some of the elements $\nu \in \mathcal{P}^p(\mathbf{q})$ in* (4.4.5)*, we replace the related term $(\beta_{0\nu} + c_\nu T)$ by the pessimistic bound* 1 *and apply random control input. In order to get a non-trivial bound in* (4.4.5)*, at least one control barrier function must be found for each $\mathbf{q} \in \mathcal{R}^p$.*

Corollary 25. *Given the result of Theorem 23, the probability that the solution process of $\mathcal{S}_J$ in* (2.3.2) *starts from any $x_0 \in L^{-1}(p)$ under control policy υ and satisfies specifications given by DFA $\mathcal{A}$ over time horizon $[0, T) \subset \mathbb{R}_{\geq 0}$ is lower-bounded by*

$$\mathbb{P}\{\varpi(\xi_{x_0\upsilon}) \models \mathcal{A}\} \geq 1 - \mathbb{P}\{\varpi(\xi_{x_0\upsilon}) \models \mathcal{A}^c\}.$$

4.4.4 Computation of Control Barrier Functions

Proving the existence of a control barrier function and finding one are in general hard problems. However, if functions f, h, g_1, g_2, r_1, and r_2 in $\mathcal{S}_J$ are polynomial with respect to their arguments and partition sets $X_i = L^{-1}(p_i), i \in \{0, 1, 2, \ldots, M\}$, are bounded semi-algebraic sets (*i.e.*, they can be represented by polynomial (in)equalities), one can formulate conditions in Theorem 20 as a sum-of-squares (SOS) optimization problem. See [13, Section 5.3.1.] for a detailed discussion on a similar approach. Having an SOS optimization problem, one can efficiently search for a polynomial control barrier function $B_\nu(x, \hat{x})$ and controller $\mathsf{u}_\nu(\hat{x})$, for any $\nu \in \mathcal{P}(\mathcal{A}_{\neg\varphi})$ as in (4.4.3) using SOSTOOLS [63] in conjunction with a semidefinite programming solver such as SeDuMi [64] while minimizing constants $\beta_{0\nu}$ and c_ν. Having values of $\beta_{0\nu}$ and c_ν for all $\nu \in \mathcal{P}(\mathcal{A}_{\neg\varphi})$, one can simply utilize results of Theorem 23 and Corollary 25 to compute a lower bound on the probability of satisfying the given specification. Note that it may not be possible in advance to obtain a probability bound that is meaningful, in such cases the order of a control barrier function needs to increase to achieve the desired probability bound.

Remark 26. *Under the assumption that sets X, X_0, and X_1 in Theorem 20 are compact and input set U is finite, one can utilize counterexample guided inductive synthesis (CEGIS) approach to search for barrier control functions for more general nonlinear functions f, h, g_1, g_2, r_1, and r_2 in* (2.3.2)*. For more detailed discussion on CEGIS approach, we kindly refer interested readers to the algorithm in [13, Section 5.3.2.].*

Computational Complexity: The number of triplets and hence the number of control barrier functions needed to be computed are bounded by $|Q|^3$, where $|Q|$ is the number of states in DFA $\mathcal{A}$. However, this is the worst-case bound and in practice, the number of control barrier functions is much smaller. In the case of sum-of-squares optimization approach, the computational complexity of finding polynomial control barrier functions depends on both the degree of polynomials and the number of state variables. One can easily see that for fixed polynomial degrees, the required computations grow polynomially with respect to the dimension of the augmented system. For the CEGIS approach, due to its iterative nature and lack of guarantee on termination, it is difficult to provide any analysis on the computational complexity.

4.5 Case Study

We consider a nonlinear Moore-Greitzer jet engine model in no-stall mode [65] as a partially-observable jump-diffusion systems by adding noise and jump terms which is given by:

$$\mathcal{S}_J : \begin{cases} \mathrm{d}\,\xi_1 &= (-\xi_2 - \frac{3}{2}\xi_1^2 - \frac{1}{2}\xi_1^3)\,\mathrm{d}\,t + 0.2\,\mathrm{d}\,W_{11t} + 0.9\,\mathrm{d}\,P_t, \\ \mathrm{d}\,\xi_2 &= (\xi_1 - \upsilon)\,\mathrm{d}\,t + 0.06\,\mathrm{d}\,W_{12t}, \\ \mathrm{d}\,y &= \xi_2\,\mathrm{d}\,t + 0.06\,\mathrm{d}\,W_{2t}, \end{cases}$$

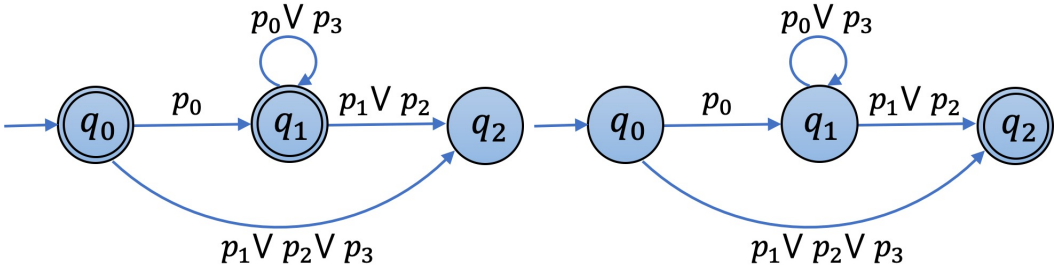

Figure 4.1: The DFA $\mathcal{A}$ representing specification (left) and the DFA $\mathcal{A}^c$ representing complement of $\mathcal{A}$ (right).

where $\xi = [\xi_1, \xi_2]^\top$, $\xi_1 = \Phi - 1$, $\xi_2 = \Psi - \psi - 2$, Φ is the mass flow, Ψ is the pressure rise, and ψ is a constant. Terms W_{11t}, W_{12t}, and W_{2t} denote the standard Brownian motions and P_t denotes the Poisson process with rate $\lambda = 5$. We consider a compact state set $X = [-1, 3] \times [-4, 4]$ and regions of interest $X_0 = [0, 1] \times [-1, 1]$, $X_1 = [-1, -0.2] \times [-4, -2.5]$, $X_2 = [1, 3] \times [2, 4]$, and $X_3 = X \setminus (X_0 \cup X_1 \cup X_2)$. The set of atomic propositions is given by $\Pi = \{p_0, p_1, p_2, p_3\}$ with labeling function $L(x_j) = p_j$ for all $x_j \in X_j$, $j \in \{0, 1, 2, 3\}$. The objective here is to compute a control policy that provides a lower bound on the probability that the trajectories of the system satisfy the specification given by the accepting language of the DFA $\mathcal{A}$ given in Figure 4.1 over finite time-horizon $[0, T = 10)$. Language of $\mathcal{A}$ entails that if we start in X_0 then the system will always stay away from X_1 or X_2. The corresponding DFA $\mathcal{A}^c$ accepting complement of $\mathcal{L}(\mathcal{A})$ is shown in Figure 4.1. Following Subsection 4.4.1, we only need to compute a control barrier function corresponding to triplet (q_0, q_1, q_2).

Now with an estimator gain in (4.2.1) as $K = [6.1394, 7.8927]^\top$, we use SOSTOOLS and SeDuMi to compute a sum-of-squares polynomial control barrier function $\mathcal{B}(x, \hat{x})$ of order 4, sum-of-square polynomials $\psi_0(x, \hat{x})$, $\psi_1(x, \hat{x})$, $\psi(x, \hat{x})$ of order 4, with total 1125 coefficients resulting in a computation time of about 15 minutes. The corresponding controller of order 2 is obtained as follows:

$$\mathsf{u}(\hat{x}) = 0.7321\hat{x}_1 - 1.8612\hat{x}_1\hat{x}_2 - 1.4356\hat{x}_2. \tag{4.5.1}$$

The values of $\beta_0 = 0.099$ and $c = 1 \times 10^{-5}$ are obtained using bisection method resulting in $\mathbb{P}\{\varpi(\xi_{x_0 v}) \models \mathcal{A}\} \geq 0.89$ for all $x_0 \in L^{-1}(p_0)$, as discussed in Subsection 4.4.4. One can see that only one controller is enough for enforcing the specification, thus we do not need any switching mechanism. Figure 4.2 shows a few trajectories starting from different initial conditions under the control policy (4.5.1).

4.6 Summary

In this chapter, we proposed a discretization-free approach for the formal controller synthesis of partially-observable jump-diffusion systems. The proposed method computes

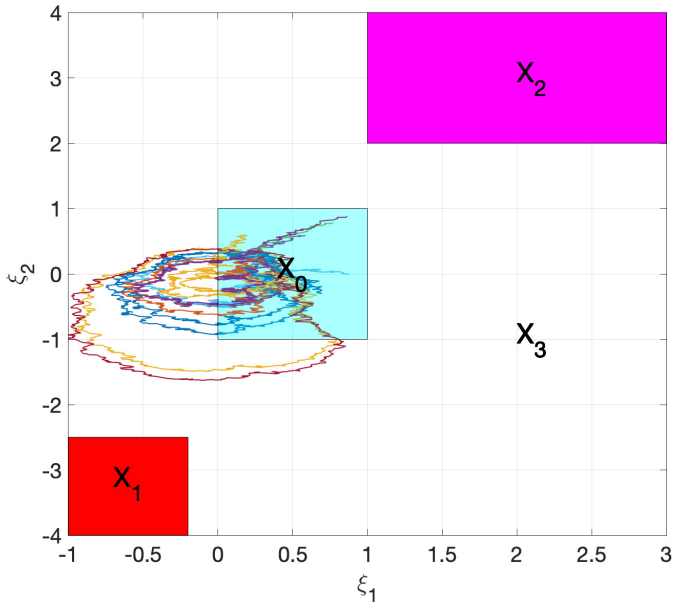

Figure 4.2: A few closed loop trajectories starting from different initial conditions in X_0 under controller (4.5.1).

a hybrid control policy together with a lower bound on the probability of satisfying complex temporal logic specifications given by the accepting language of DFA $\mathcal{A}$ over a finite-time horizon. This is achieved by constructing control barrier functions over an augmented system consisting of both the system and the estimator. As a result, the probability bound is computed without requiring any prior information of the estimation accuracy.

Chapter 5

Compositional Construction of Safety Controllers for Networks of Continuous-Space POMDPs

In this chapter, we propose a compositional framework for the synthesis of safety controllers for networks of partially-observable discrete-time stochastic control systems (a.k.a. continuous-space POMDPs). Given an estimator, we utilize a discretization-free approach to synthesize controllers ensuring safety specifications over finite time horizons. The proposed framework is based on a notion of so-called *local control barrier functions* computed for subsystems in two different ways. In the first scheme, no prior knowledge of estimation accuracy is needed. The second framework utilizes a probability bound on the estimation accuracy using a notion of so-called *stochastic simulation functions*. In both proposed schemes, we derive sufficient small-gain type conditions in order to compositionally construct control barrier functions for interconnected POMDPs using local barrier functions computed for subsystems. The constructed control barrier functions for the overall networks enable us to compute lower bounds on the probabilities that the interconnected POMDPs avoid certain unsafe regions in finite time horizons. We demonstrate the effectiveness of our proposed approaches by applying them to an adaptive cruise control problem.

5.1 Introduction

Large-scale stochastic systems have received significant attentions in the past few years due to their broad applications in modeling many engineering systems such as power grids, road traffic networks, and industrial control systems, to name a few. Guaranteeing safety and reliability of such complex systems in a formal as well as time- and cost-effective way has always been very challenging. In the previous chapters, we presented discretization-free approaches based on *control barrier functions* in order to formally synthesize controllers

satisfying complex logic specifications such as safety and those that can be expressed as deterministic finite automata. Though promising, the computational complexity of the proposed methods will prevent us from applying them to large-scale systems. One way to address this issue is to utilize compositional approaches.

5.1.1 Related Literature

Discretization-based and discretization-free compositional techniques have both been utilized for the formal synthesis of controllers for large-scale systems. By viewing large-scale systems as the interconnections of reasonably-sized and properly interconnected subsystems, one only deals with the analysis and design of the subsystems instead of the overall interconnected system.

Compositional abstraction-based approaches

Several compositional abstraction-based approaches were proposed to deal with the aforementioned scalability issue, where compositional techniques have been used to construct finite abstractions of interconnected systems based on abstractions of smaller subsystems. See the results in [8, 9, 10, 66, 67, 68, 69, 70] for more details.

Compositional approaches based on control barrier functions

As we have discussed in chapters 3 and 4, control barrier functions serve as a powerful tool to formally synthesize safety controllers for partially-observable systems. However, when dealing with large scale systems, the monolithic view of the proposed approaches results in high computational complexity. To this end, compositional construction of control barrier functions for non-stochastic systems is presented in [14]. Moreover, compositional construction of control barrier functions for continuous and stochastic hybrid systems is presented in [71, 72, 73, 74, 75].

Unfortunately, all the above-mentioned literatures on both discretization and discretization-free techniques assume that full state information is available, which is not the case in many practical applications. Taking this limitation into account, the results in [76, 77, 78] study verification of partially-observable Markov decision processes with finite state and action spaces (finite POMDPs) using barrier certificates. A controller synthesis in multi-agent POMDPs via discrete-time barrier functions to enforce safety is proposed in [79] and [27].

5.1.2 Contribution

The contents of this chapter have been published in the IEEE Transactions on Control of Network Systems [80]. It is a joint work with Prof. Abolfazl Lavaei and Prof. Majid Zamani. The author of the thesis has established the results and written the draft. Abolfazl Lavaei contributed to the initial discussions, some results, the revision of the draft, and mentoring. Majid Zamani supervised the work.

In this chapter, we propose a compositional approach for the construction of control

barrier functions for partially-observable discrete-time stochastic control systems (a.k.a. continuous-space POMDPs). In particular, by considering a large-scale partially-observable stochastic control system as an interconnection of lower-dimensional subsystems, we compute so-called *local control barrier functions* for subsystems along with the corresponding local controllers. We then utilize local control barrier functions of subsystems to compositionally construct an overall control barrier function for the overall interconnected system.

5.2 Preliminaries and Problem Definition

We now formally define the main synthesis problem we are interested to solve in this chapter.

Problem 27. *Given an interconnection of partially observable stochastic control systems, synthesize a decentralized safety controller ensuring that the trajectories of the interconnected system will not enter a given unsafe region over a finite time horizon with some lower bound on the probability of satisfaction.*

Finding a solution to Problem 27 (if existing) is difficult in general. In this chapter, we provide a computational approach which is *sound* but not *complete* in solving the synthesis problem. This means if our proposed method fails to find a controller, then a controller satisfying the safety specification may or may not exist. Here, we develop a compositional controller synthesis scheme for networks of partially-observable stochastic control systems based on barrier functions. By requiring some small-gain type conditions, we compositionally construct a control barrier function for the interconnected system based on local barrier functions of subsystems.

We propose two approaches, based on the results in Chapter 3 and Chapter 4, for the construction of control barrier functions. In the first one, local control barrier functions are defined over augmented systems consisting of subsystems and their estimators. This formulation makes it possible to search for local control barrier functions, and the overall one, without requiring explicitly the accuracies of the estimators. In the second framework, local control barrier functions are constructed using the estimators' dynamics (without augmenting them with the subsystems' dynamics) where we utilize a notion of so-called *stochastic simulation functions* to compute a probabilistic bound on the estimation accuracy. We propose a sum-of-squares (SOS) optimization approach to search for local control barrier functions in both approaches, and accordingly, to compute the corresponding controllers. In order to illustrate the effectiveness of our proposed results, we apply both approaches to an adaptive cruise control problem.

For the sake of controller synthesis using control barrier functions which are explained later in detail, we raise the following assumption on the existence of an estimator that estimates the state of the PO-dt-SCS in (2.3.5).

Assumption 4. *Consider a PO-dt-SCS* $\Sigma_S = (X, U, W, \varsigma_1, f, Y_1, Y_2, h_1, h_2, \varsigma_2)$. *States of* Σ_S *in* (2.3.5) *can be estimated by a proper estimator* $\widehat{\Sigma}_S$ *which is characterized by the tuple*

$\widehat{\Sigma}_S = (X, U, W, \hat{f}, Y_1, Y_2, h_1)$ *and represented in the following form:*

$$\widehat{\Sigma}_S : \begin{cases} \hat{x}(k+1) = \hat{f}(\hat{x}(k), \upsilon(k), \hat{w}(k), y_2(k)), \\ \hat{y}_1(k) = h_1(\hat{x}(k)), \end{cases} \tag{5.2.1}$$

where υ and y_2 are external input and output signals of Σ_S and $\hat{w}$ is the internal input signal coming from other estimators. We explain later how $\hat{w}$ is being fed by the estimators of other neighbouring subsystems.

There exist numerous results in the relevant literature for the design of the estimator in (5.2.1) *for different classes of stochastic systems (cf. [81, 82, 83, 84]).*

In the next section, we introduce notions of local control barrier functions (LCBF) and control barrier functions (CBF) for respectively POMDPs (with both internal and external inputs) and interconnected POMDPs (without internal inputs and outputs).

5.3 (Local) Control Barrier Functions

First, we define (local) control barrier functions ((L)CBF) over an augmented system consisting of the stochastic (sub)system's and its estimator's dynamics. This formulation enables one to search for (local) control barrier functions with no prior knowledge of the estimation accuracy. Second, we formulate (local) control barrier functions over the estimator's dynamics (without augmenting them with the subsystem's dynamics) by utilizing a given probability bound on the estimation accuracy computed via a notion of so-called stochastic simulation functions.

5.3.1 Notions of (L)CBF without considering the estimation accuracy

Here, we first define the augmented process $\big[x(k); \hat{x}(k)\big]$, where $x(k)$ and $\hat{x}(k)$ are the solution processes of subsystems Σ_S in (2.3.5) and their estimators $\widehat{\Sigma}_S$ in (5.2.1), respectively. The corresponding augmented stochastic subsystem $\widetilde{\Sigma}_S$ can be defined as:

$$\widetilde{\Sigma}_S : \begin{bmatrix} x(k+1) \\ \hat{x}(k+1) \end{bmatrix} = \begin{bmatrix} f(x(k), \upsilon(k), w(k), \varsigma_1(k)) \\ \hat{f}(\hat{x}(k), \upsilon(k), \hat{w}(k), y_2(k)) \end{bmatrix}. \tag{5.3.1}$$

Now, the local control barrier function is defined for system $\widetilde{\Sigma}_S$ in (5.3.1).

Remark 28. *The use of the augmented system $\widetilde{\Sigma}_S$ will allow us to provide one of the main results of the chapter without requiring explicitly any prior knowledge of the probabilistic distance between the actual states and their estimations. This will provide flexibility in designing estimators by means of any existing method.*

We now formally define local control barrier functions constructed over the augmented system $\widetilde{\Sigma}_S$.

Definition 29. *Consider a POMDP Σ_S in (2.3.5), its estimator $\widehat{\Sigma}_S$ in (5.2.1), and the resulting augmented system $\widetilde{\Sigma}_S$ in (5.3.1). Let $X_0, X_1 \subseteq X$ represent some initial and unsafe regions, respectively. A function $\mathcal{B} : X \times X \to \mathbb{R}_{\geq 0}$ is called a local control barrier function (LCBF) for $\widetilde{\Sigma}_S$ if there exist constants $\bar{c}, \bar{\beta}_0 \in \mathbb{R}_{\geq 0}$ and $\bar{\beta}_1 \in \mathbb{R}_{>0}$, such that*

- $\forall (x, \hat{x}) \in X \times X$,
$$\mathcal{B}(x, \hat{x}) \geq \alpha(\| \begin{bmatrix} h_1(x) \\ h_1(\hat{x}) \end{bmatrix} \|^2), \tag{5.3.2}$$
- $\forall (x, \hat{x}) \in X_0 \times X_0$,
$$\mathcal{B}(x, \hat{x}) \leq \bar{\beta}_0, \tag{5.3.3}$$
- $\forall (x, \hat{x}) \in X_1 \times X$,
$$\mathcal{B}(x, \hat{x}) \geq \bar{\beta}_1, \tag{5.3.4}$$
- $\forall \hat{x}(k) \in X$, $\forall \hat{w}(k) \in W$, $\exists \upsilon(k) \in U$, *such that* $\forall x(k) \in X$, $\forall w(k) \in W$,

$$\begin{aligned} &\mathbb{E}\Big[\mathcal{B}\big(f(x(k), \upsilon(k), w(k), \varsigma_1(k)), \hat{f}(\hat{x}(k), \upsilon(k), \hat{w}(k), y_2(k))\big) \,\Big|\, x(k), \hat{x}(k), \upsilon(k), w(k), \hat{w}(k)\Big] \\ &\quad \leq \max\Big\{\bar{\kappa}\mathcal{B}(x(k), \hat{x}(k)), \rho(\| \begin{bmatrix} w(k) \\ \hat{w}(k) \end{bmatrix} \|^2), \bar{c}\Big\}, \end{aligned} \tag{5.3.5}$$

for some $\bar{\kappa} \in \mathcal{K}_\infty$, with $\bar{\kappa} < \mathcal{I}_d$, $\alpha \in \mathcal{K}_\infty$, and $\rho \in \mathcal{K}_\infty \cup \{0\}$.

Definition 29 can also be stated for interconnected systems without internal inputs and outputs by eliminating all the terms related to the internal input w, its estimation $\hat{w}$, internal output $h_1(x)$, and its estimation $h_1(\hat{x})$ as defined below.

Definition 30. *Consider an (interconnected) POMDP $\Sigma_S = (X, U, \varsigma_1, f, Y, h, \varsigma_2)$, its estimator $\widehat{\Sigma}_S$ also without internal inputs and outputs, and the augmented system $\widetilde{\Sigma}_S = [\Sigma_S; \widehat{\Sigma}_S]$. Let $X_0, X_1 \subseteq X$, respectively, represent initial and unsafe regions. A function $\mathcal{B} : X \times X \to \mathbb{R}_{\geq 0}$ is called a control barrier function (CBF) for $\widetilde{\Sigma}_S$ if there exist constants $c, \beta_0 \in \mathbb{R}_{\geq 0}$ and $\beta_1 \in \mathbb{R}_{>0}$ such that $\beta_0 < \beta_1$, and*

- $\forall (x, \hat{x}) \in X_0 \times X_0$,
$$\mathcal{B}(x, \hat{x}) \leq \beta_0, \tag{5.3.6}$$
- $\forall (x, \hat{x}) \in X_1 \times X$,
$$\mathcal{B}(x, \hat{x}) \geq \beta_1, \tag{5.3.7}$$
- *and* $\forall \hat{x}(k) \in X$, $\exists \upsilon(k) \in U$, *such that* $\forall x(k) \in X$,

$$\begin{aligned} &\mathbb{E}\Big[\mathcal{B}\big(f(x(k), \upsilon(k), \varsigma_1(k)), \hat{f}(\hat{x}(k), \upsilon(k), y(k))\big) \,\Big|\, x(k), \hat{x}(k), \upsilon(k)\Big] \\ &\quad \leq \max\big\{\kappa\mathcal{B}(x(k), \hat{x}(k)), c\big\}, \end{aligned} \tag{5.3.8}$$

for some $\kappa \in \mathcal{K}_\infty$, with $\kappa < \mathcal{I}_d$.

Remark 31. *Note that the compositionality conditions in this chapter are based on so-called max-type small-gain approach. Thus, the upper bound in* (5.3.8) *is in the max form and the overall CBF is the maximum of LCBF of subsystems under some scaling (this is explained further in Section 5.5).*

Remark 32. *Note that we need the condition* $\beta_0 < \beta_1$ *(*i.e., $X_0 \cap X_1 = \emptyset$*) in order to provide a meaningful probability in Theorem 33 later. This requirement is only for the interconnected system and not for subsystems. In particular, LCBFs are mainly utilized for the compositional construction of CBFs over interconnected systems and are not directly employed for ensuring the probability of safety satisfaction. The above definition associates a controller* $\mathsf{u} : X \to U$ *to a CBF, where* X *here is the state set of the estimator* $\widehat{\Sigma}_S$*. Definition 30 gives such a controller according to the existential quantifier over the input for any estimator's state* $\hat{x} \in X$*.*

The next theorem shows the usefulness of having a CBF to quantify an upper bound on the exit probability (*i.e.,* the probability that the solution process of the interconnected system reaches the unsafe region in a finite time horizon) of POMDP (without internal inputs and outputs).

Theorem 33. *Let* $\Sigma_S = (X, U, \varsigma_1, f, Y, h, \varsigma_2)$ *be a POMDP (without internal inputs and outputs) and* $\widehat{\Sigma}_S$ *be its corresponding estimator. Suppose* $\mathcal{B}$ *is a CBF according to Definition 30 with a controller* $\mathsf{u} : X \to U$*. Then, the probability that the solution process of* Σ_S *starts from any initial states* $x(0) = x_0 \in X_0$ *and reaches* X_1 *under the controller* u *within a time horizon* $[0, T_d]$ *is formally upper bounded as*

$$\mathbb{P}\Big[x_{x_0\upsilon}(k) \in X_1 \text{ for some } k \in [0, T_d] \;\Big|\; x_0, \upsilon\Big] \leq \delta, \tag{5.3.9}$$

where,

$$\delta := \begin{cases} 1 - (1 - \frac{\beta_0}{\beta_1})(1 - \frac{c}{\beta_1})^{T_d}, & \text{if } \beta_1 \geq \frac{c}{1-\kappa}, \\ \\ \frac{\beta_0}{\beta_1}\kappa^{T_d} + (\frac{c}{(1-\kappa)\beta_1})(1 - \kappa^{T_d}), & \text{if } \beta_1 < \frac{c}{1-\kappa}. \end{cases} \tag{5.3.10}$$

Proof. According to condition (5.3.7), $X_1 \times X \subseteq \{(x, \hat{x}) \in X \times X \mid \mathcal{B}(x, \hat{x}) \geq \beta_1\}$. Then we have

$$\begin{aligned} &\mathbb{P}\big[x_{x_0\upsilon}(k) \in X_1 \wedge \hat{x}_{\hat{x}_0\upsilon}(k) \in X \text{ for some } k \in [0, T_d] \;\big|\; x_0, \hat{x}_0, \upsilon\big] \\ &\quad \leq \mathbb{P}\big[\sup_{0 \leq k \leq T_d} \mathcal{B}(x_{x_0\upsilon}(k), \hat{x}_{\hat{x}_0\upsilon}(k)) \geq \beta_1 \;\big|\; x_0, \hat{x}_0, \upsilon\big] \leq \delta. \end{aligned} \tag{5.3.11}$$

The proposed bounds in (5.3.9) follow directly by applying [39, Theorem 3, Chapter III] to the above inequality and employing conditions (5.3.8) and (5.3.6), respectively. Inequality

(5.3.11) is obtained by utilizing the result of [33, Theorem 1]. Now we get

$$\begin{aligned}&\mathbb{P}\big[x_{x_0\upsilon}(k) \in X_1 \wedge \hat{x}_{\hat{x}_0\upsilon}(k) \in X \text{ for some } k \in [0, T_d] \;\big|\; x_0, \hat{x}_0, \upsilon\big]\\ &\leq \mathbb{P}\big[x_{x_0\upsilon}(k) \in X_1 \text{ for some } k \in [0, T_d] \mid x_0, \upsilon\big]\\ &+ \mathbb{P}\big[\hat{x}_{\hat{x}_0\upsilon}(k) \in X \text{ for some } k \in [0, T_d] \;\big|\; \hat{x}_0, \upsilon\big]\\ &- \mathbb{P}\big[x_{x_0\upsilon}(k) \in X_1 \vee \hat{x}_{\hat{x}_0\upsilon}(k) \in X \text{ for some } k \in [0, T_d] \;\big|\; x_0, \hat{x}_0, \upsilon\big].\end{aligned}$$

Since, the second and last terms trivially hold with probability 1, one has

$$\begin{aligned}&\mathbb{P}\big[x_{x_0\upsilon}(k) \in X_1 \wedge \hat{x}_{\hat{x}_0\upsilon}(k) \in X \text{ for some } k \in [0, T_d] \;\big|\; x_0, \hat{x}_0, \upsilon\big]\\ &\leq \mathbb{P}\big[x_{x_0\upsilon}(k) \in X_1 \text{ for some } k \in [0, T_d] \;\big|\; x_0, \upsilon\big].\end{aligned}$$

Now, since the right term of the conjunction (i.e., $\wedge$) holds for all time, the inequality above becomes an equality and one gets $\mathbb{P}\big[x_{x_0\upsilon}(k) \in X_1 \text{ for some } k \in [0, T_d] \;\big|\; x_0, \upsilon\big] \leq \delta$ which concludes the proof. □

Remark 34. *Utilizing the augmented system $\widetilde{\Sigma}_S$ as in* (5.3.1) *provides us with the results in Theorem 33 without requiring the estimation accuracy explicitly. This allows more flexibility in designing the estimator and potentially results in tighter upper bounds.*

In the next subsection, we formulate control barrier functions only over the estimators' dynamics by utilizing a probability bound on the estimation accuracy.

5.3.2 Notions of (L)CBF by considering the estimation accuracy

Given an estimator with a probabilistic guarantee on the accuracy of the estimation, we propose an approach to construct a CBF defined only over the states of the estimator $\widehat{\Sigma}_S$. For a given time horizon T_d, we assume the probabilistic bound on the accuracy of the estimator is given by [31]:

$$\begin{aligned}&\forall \epsilon > 0, \exists \theta \in (0, 1], \text{ such that}\\ &\mathbb{P}\Big[\sup_{0 \leq k \leq T_d} \|x_{x_0\upsilon}(k) - \hat{x}_{\hat{x}_0\upsilon}(k)\| < \epsilon \,\Big|\, x_0, \hat{x}_0, \upsilon\Big] \geq 1 - \theta,\end{aligned} \tag{5.3.12}$$

for any $x_0, \hat{x}_0 \in X$ and any $\upsilon \in \mathcal{U}$. In order to quantify the distance (a.k.a. error) between a system's state and its estimation, we employ notions of so-called stochastic (pseudo)-simulation functions. To do so, we first introduce stochastic pseudo-simulation functions (SPSF) for POMDPs with both internal and external inputs. We then define stochastic simulation functions (SSF) for interconnected POMDPs without internal inputs and outputs.

Definition 35. *Consider a POMDP Σ_S in* (2.3.5) *and its corresponding estimator $\widehat{\Sigma}_S$ in* (5.2.1)*. A function $\boldsymbol{\phi} : X \times X \to \mathbb{R}_{\geq 0}$ is called a stochastic pseudo-simulation function (SPSF) from $\widehat{\Sigma}_S$ to Σ_S if*

1. $\forall x \in X, \forall \hat{x} \in X$,
$$\varepsilon(\|x - \hat{x}\|) \leq \boldsymbol{\phi}(x, \hat{x}),$$
2. $\forall \hat{x}(k) \in X, \forall \hat{w}(k) \in W, \forall \upsilon(k) \in U$, $\forall x(k) \in X$, *and* $\forall w(k) \in W$,
$$\mathbb{E}\Big[\boldsymbol{\phi}\big(f(x(k), \upsilon(k), w(k), \varsigma_1(k)), \hat{f}(\hat{x}(k), \upsilon(k), \hat{w}(k), y_2(k))\big) \,\Big|\, x(k), \hat{x}(k), \upsilon(k), w(k), \hat{w}(k)\Big] \leq \max\big\{\bar{c}_2 \boldsymbol{\phi}(x(k), \hat{x}(k)), \varrho(\|w(k) - \hat{w}(k)\|), \bar{c}_1\big\},$$

for some $\bar{c}_2 \in \mathcal{K}_\infty$, *with* $\bar{c}_2 < \mathcal{I}_d$, $\varepsilon \in \mathcal{K}_\infty$, $\varrho \in \mathcal{K}_\infty \cup \{0\}$, *and* $\bar{c}_1 \in \mathbb{R}_{\geq 0}$.

Definition 35 can also be stated for POMDPs without internal inputs and outputs by eliminating all the terms related to the internal input w and its estimation $\hat{w}$ as defined below.

Definition 36. *Consider an (interconnected) POMDP* $\Sigma_S = (X, U, \varsigma_1, f, Y, h, \varsigma_2)$ *and its estimator* $\widehat{\Sigma}_S$. *A function* $\boldsymbol{\phi} : X \times X \to \mathbb{R}_{\geq 0}$ *is called a stochastic simulation function (SSF) from* $\widehat{\Sigma}_S$ *to* Σ_S *if*

1. $\forall x \in X, \forall \hat{x} \in X$,
$$\varepsilon(\|x - \hat{x}\|) \leq \boldsymbol{\phi}(x, \hat{x}),$$
2. $\forall \hat{x}(k) \in X, \forall \upsilon(k) \in U$, *and* $\forall x(k) \in X$,
$$\mathbb{E}\Big[\boldsymbol{\phi}\big(f(x(k), \upsilon(k), \varsigma_1(k)), \hat{f}(\hat{x}(k), \upsilon(k), y(k))\big) \,\Big|\, x(k), \hat{x}(k), \upsilon(k)\Big] \leq \max\big\{c_2 \boldsymbol{\phi}(x(k), \hat{x}(k)), c_1\big\},$$

for some $c_2 \in \mathcal{K}_\infty$, *with* $c_2 < \mathcal{I}_d$, $\varepsilon \in \mathcal{K}_\infty$, *and* $c_1 \in \mathbb{R}_{\geq 0}$.

The next theorem shows how an SSF can be employed to obtain the probability bound on the estimation accuracy.

Theorem 37. *Consider a POMDP* Σ_S *in* (2.3.6), *its estimator* $\widehat{\Sigma}_S$ *in* (5.2.1) *(without internal inputs and outputs), and* $\epsilon > 0$. *Suppose* $\boldsymbol{\phi}$ *is an SSF from* $\widehat{\Sigma}_S$ *to* Σ_S. *For any* $\upsilon \in \mathcal{U}$, *and for any random variables* x_0 *and* $\hat{x}_0$ *as initial states of* Σ_S *and* $\widehat{\Sigma}_S$, *respectively, the following inequality holds:*
$$\mathbb{P}\Big[\sup_{0 \leq k \leq T_d} \|x_{x_0\upsilon}(k) - \hat{x}_{\hat{x}_0\upsilon}(k)\| \geq \epsilon \,\Big|\, x_0, \hat{x}_0, \upsilon\Big] \leq \theta,$$

where,
$$\theta := \begin{cases} 1 - (1 - \frac{\boldsymbol{\phi}(x_0, \hat{x}_0)}{\varepsilon(\epsilon)})(1 - \frac{c_1}{\varepsilon(\epsilon)})^{T_d}, & \text{if } \varepsilon(\epsilon) \geq \frac{c_1}{1 - c_2}, \\ (\frac{\boldsymbol{\phi}(x_0, \hat{x}_0)}{\varepsilon(\epsilon)}) c_2^{T_d} + (\frac{c_1}{(1 - c_2)\varepsilon(\epsilon)})(1 - c_2^{T_d}), & \text{if } \varepsilon(\epsilon) < \frac{c_1}{1 - c_2}. \end{cases} \tag{5.3.13}$$

Proof. Since $\boldsymbol{\phi}$ is a stochastic pseudo-simulation function from $\widehat{\Sigma}_S$ to Σ_S, one has

$$\begin{aligned}
&\mathbb{P}\Big[\sup_{0\leq k\leq T_d}\|x_{x_0\upsilon}(k)-\hat{x}_{\hat{x}_0\upsilon}(k)\|\geq\epsilon\;\Big|\;x_0,\hat{x}_0,\upsilon\Big]\\
&=\mathbb{P}\Big[\sup_{0\leq k\leq T_d}\varepsilon(\|x_{x_0\upsilon}(k)-\hat{x}_{\hat{x}_0\upsilon}(k)\|)\geq\varepsilon(\epsilon)\;\Big|\;x_0,\hat{x}_0,\upsilon\Big]\\
&\leq\mathbb{P}\Big[\sup_{0\leq k\leq T_d}\boldsymbol{\phi}(x_{x_0\upsilon}(k),\hat{x}_{\hat{x}_0\upsilon}(k))\geq\varepsilon(\epsilon)\;\Big|\;x_0,\hat{x}_0,\upsilon\Big]\leq\theta.
\end{aligned}$$

The equality holds due to the fact that α_ϕ is a $\mathcal{K}_\infty$ function. The second inequality holds based on the first condition of Definition 36, and the last inequality follows from the result in [39, Theorem 1]. □

We now propose our second formulation of control barrier functions defined only over the estimators' dynamics as the following.

Definition 38. *Consider a POMDP Σ_S as in* (2.3.5)*, its estimator $\widehat{\Sigma}_S$, and $\epsilon>0$. Let $X_0,X_1\subseteq X$ denote respectively initial and unsafe sets. Let us define $X_1^\epsilon:=\{\hat{x}\in X\mid\exists x\in X_1,\|\hat{x}-x\|\leq\epsilon\}$ (*i.e., *unsafe set for $\widehat{\Sigma}_S$). A function $\mathcal{B}:X\to\mathbb{R}_{\geq0}$ is called a local control barrier function (LCBF) for $\widehat{\Sigma}_S$ if there exist constants $\bar{c},\bar{\beta}_0\in\mathbb{R}_{\geq0}$ and $\bar{\beta}_1\in\mathbb{R}_{>0}$, such that*

- $\forall x\in X$,
$$\mathcal{B}(x)\geq\alpha(\|h_1(x)\|^2),\tag{5.3.14}$$
- $\forall x\in X_0$,
$$\mathcal{B}(x)\leq\bar{\beta}_0,\tag{5.3.15}$$
- $\forall x\in X_1^\epsilon$,
$$\mathcal{B}(x)\geq\bar{\beta}_1,\tag{5.3.16}$$
- *and $\forall\hat{x}(k)\in X$, $\forall\hat{w}(k)\in W$, $\exists\upsilon(k)\in U$, such that $\forall x(k)\in X$,*
$$\begin{aligned}
&\mathbb{E}\Big[\mathcal{B}\big(\hat{f}(\hat{x}(k),\upsilon(k),\hat{w}(k),h_2(x(k),\varsigma_2(k)))\big)\mid\hat{x}(k),\upsilon(k),\hat{w}(k),x(k)\Big]\\
&\quad\leq\max\big\{\bar{\kappa}\mathcal{B}(\hat{x}(k)),\rho(\|\hat{w}(k)\|^2),\varkappa(\|x(k)-\hat{x}(k)\|^2),\bar{c}\big\},
\end{aligned}\tag{5.3.17}$$

for some $\bar{\kappa}\in\mathcal{K}_\infty$, with $\bar{\kappa}<\mathcal{I}_d$, $\alpha,\varkappa\in\mathcal{K}_\infty$, and $\rho\in\mathcal{K}_\infty\cup\{0\}$.

We now modify Definition 38 and present it for the interconnected POMDPs as the following.

Definition 39. *Consider an (interconnected) POMDP $\Sigma_S=(X,U,\varsigma_1,f,Y,h,\varsigma_2)$, its estimator $\widehat{\Sigma}_S$ without internal inputs and outputs and $\epsilon>0$. Let $X_0,X_1\subseteq X$ denote respectively initial and unsafe sets. Let us define $X_1^\epsilon:=\{\hat{x}\in X\mid\exists x\in X_1,\|\hat{x}-x\|\leq\epsilon\}$. A function $\mathcal{B}:X\to\mathbb{R}_{\geq0}$ is called a control barrier function for $\widehat{\Sigma}_S$ if there exist constants $c,\beta_0\in\mathbb{R}_{\geq0}$ and $\beta_1\in\mathbb{R}_{>0}$ such that $\beta_0<\beta_1$ and*

- $\forall x \in X_0$,
$$\mathcal{B}(x) \leq \beta_0,$$
- $\forall x \in X_1^\epsilon$,
$$\mathcal{B}(x) \geq \beta_1,$$
- *and* $\forall \hat{x}(k) \in X$, $\exists \upsilon(k) \in U$, *such that* $\forall x(k) \in X$,
$$\mathbb{E}\Big[\mathcal{B}\big(\hat{f}(\hat{x}(k), \upsilon(k), h(x(k), \varsigma_2(k)))\big) \mid \hat{x}(k), \upsilon(k), x(k)\Big] \leq \max\big\{\kappa\mathcal{B}(\hat{x}(k)), \varkappa(\|x(k) - \hat{x}(k)\|^2), c\big\},$$

for some $\kappa \in \mathcal{K}_\infty$, *with* $\kappa < \mathcal{I}_d$, *and* $\varkappa \in \mathcal{K}_\infty$.

In the next Theorem, we provide an upper bound on the exit probability of POMDP using the estimation accuracy.

Theorem 40. *Let* $\Sigma_S = (X, U, \varsigma_1, f, Y, h, \varsigma_2)$ *be a POMDP without internal inputs and outputs,* $\widehat{\Sigma}_S$ *be its corresponding estimator with an accuracy* ϵ *and a probability bound on the estimation accuracy* θ, *as in Theorem 37. Suppose* $\mathcal{B}$ *is a CBF for* $\widehat{\Sigma}_S$ *as in Definition 39 with a controller* $\mathsf{u} : X \to U$. *Then, the probability that the solution process of* Σ_S *starts from any initial state* $x(0) = x_0 \in X_0$ *and not reaches* X_1 *under the controller* u *within a time horizon* $[0, T_d]$ *is lower bounded as*

$$\mathbb{P}\Big[x_{x_0\upsilon}(k) \notin X_1 \text{ for all } k \in [0, T_d] \;\Big|\; x_0, \upsilon\Big] \geq (1 - \delta)(1 - \theta), \tag{5.3.18}$$

where θ *is computed as in* (5.3.13), *and* δ *is computed as in* (5.3.10) *with* c *in* (5.3.10) *being replaced with a constant* $\hat{c} \geq 0$ *satisfying* $\hat{c} \geq \varkappa(\|\epsilon\|^2) + c$.

Proof. Given $x_0, \hat{x}_0 \in X_0$, let us define the events $A_1 := \big[x_{x_0\upsilon}(k) \in X_1 \text{ for some } k \in [0, T_d]\big]$, $A_2 := \big[\hat{x}_{\hat{x}_0\upsilon}(k) \in X_1^\epsilon \text{ for some } k \in [0, T_d]\big]$ and $A_3 := \big[\sup_{0\leq k\leq T_d} \|x_{x_0\upsilon}(k) - \hat{x}_{\hat{x}_0\upsilon}(k)\| \leq \epsilon\big]$. Then, we have

$$\mathbb{P}\big[\bar{A}_1\big] \overset{(*)}{=} \mathbb{P}\big[\bar{A}_2 \cap A_3\big] = \mathbb{P}\big[\bar{A}_2 \,|\, A_3\big]\mathbb{P}\big[A_3\big] \overset{(**)}{\geq} (1 - \delta)(1 - \theta),$$

where $\bar{A}_i$ is the complement of event A_i for $i \in \{1, 2\}$, and $\mathbb{P}[\bar{A}_2 \mid A_3]$ is conditional probability. The first equality $(*)$ comes from the definition of X_1^ϵ being an $\epsilon-$inflated version of X_1. Notice that in the last inequality $(**)$, the term $\mathbb{P}[\bar{A}_2 \mid A_3]$ is lower bounded by $(1 - \delta)$, since if A_3 holds, $\varkappa(\|x(k) - \hat{x}(k)\|^2)$ in Definition 39 will be upper bounded by $\varkappa(\|\epsilon\|^2)$. Furthermore, the term $\mathbb{P}[A_3]$ is lower bounded by $(1 - \theta)$ by Theorem 37. This concludes the proof. □

Remark 41. *Note that the first proposed approach does not require a prior knowledge of the estimation accuracy, and accordingly, it gives the user more flexibility on the estimator design. Moreover, in the first approach the computation of the exit probability can be done in one shot without utilizing SSFs and, hence, be less conservative. However, the computational complexity in the first approach is more than the second one since the control barrier function should be constructed over the augmented system.*

In the next sections, we analyze networks of POMDP and discuss under which conditions one can construct a CBF of an interconnected system based on LCBF of its subsystems.

5.4 Interconnected POMDP

We consider a collection of partially-observable stochastic control subsystems and their estimators as

$$\begin{aligned}\Sigma_{S_i} &= (X_i, U_i, W_i, \varsigma_{1i}, f_i, Y_{1_i}, Y_{2_i}, h_{1_i}, h_{2_i}, \varsigma_{2_i}),\\ \widehat{\Sigma}_{S_i} &= (X_i, U_i, W_i, \hat{f}_i, Y_{1_i}, Y_{2_i}, h_{1_i}),\ i \in \{1, \dots, N\},\end{aligned}$$

where internal inputs and outputs are partitioned as

$$\begin{aligned}w_i &= \big[w_{i1}; \dots; w_{i(i-1)}; w_{i(i+1)}; \dots; w_{iN}\big],\\ y_{1_i} &= \big[y_{1_{i1}}; \dots y_{1_{i(i-1)}}; y_{1_{i(i+1)}}; \dots; y_{1_{iN}}\big],\end{aligned} \tag{5.4.1}$$

and their internal output spaces and functions are of the form

$$\begin{aligned}Y_{1_i} &= \prod_{j=1, j\neq i}^{N} Y_{1_{ij}},\\ h_{1_i}(x_i) &= [h_{1_{i1}}(x_i); \dots; h_{1_{i(i-1)}}(x_i); h_{1_{i(i+1)}}(x_i); \dots h_{1_{iN}}(x_i)].\end{aligned} \tag{5.4.2}$$

Furthermore, the internal input and output of the estimators are also partitioned similar to (5.4.1) and (5.4.2).

Outputs $y_{1_{ij}}$ with $i \neq j$ are *internal* outputs which are employed for the sake of interconnections. If there is a connection from Σ_{S_j} to Σ_{S_i}, we assume that w_{ij} is equal to $y_{1_{ji}}$. Otherwise, the connecting output function is identically zero, *i.e.,* $h_{1_{ji}} \equiv 0$. The same interconnections hold for the estimators. If there is a connection from $\widehat{\Sigma}_{S_j}$ to $\widehat{\Sigma}_{S_i}$, we assume that $\hat{w}_{ij}$ is equal to $\hat{y}_{1_{ji}}$. Otherwise, the connecting output function is identically zero, *i.e.,* $h_{1_{ji}} \equiv 0$. Now we define interconnected partially-observable stochastic control systems.

Definition 42. *Consider $N \in \mathbb{N}_{\geq 1}$ POMDPs $\Sigma_{S_i} = (X_i, U_i, W_i, \varsigma_{1_i}, f_i, Y_{1_i}, Y_{2_i}, h_{1_i}, h_{2_i}, \varsigma_{2_i})$, $i \in \{1, \dots, N\}$, with the input-output configuration as in* (5.4.1)-(5.4.2)*. The interconnection of Σ_{S_i}, for any $i \in \{1, \dots N\}$, is the interconnected POMDP $\Sigma_S = (X, U, \varsigma_1, f, Y, h, \varsigma_2)$, denoted by $\mathcal{I}(\Sigma_{S_1}, \dots, \Sigma_{S_N})$, such that $X := \prod_{i=1}^{N} X_i$, $U := \prod_{i=1}^{N} U_i$, $\varsigma_1 = \big[\varsigma_{1_1}; \cdots; \varsigma_{1_N}\big]$,*

$f := \prod_{i=1}^{N} f_i$, $Y := \prod_{i=1}^{N} Y_i$, $h := \prod_{i=1}^{N} h_i$, *and* $\varsigma_2 = \left[\varsigma_{2_1}; \cdots; \varsigma_{2_N}\right]$, *subjected to the following constraint:*

$$\forall i, j \in \{1, \ldots, N\}, i \neq j: \quad w_{ji} = y_{1_{ij}}, \quad Y_{1_{ij}} \subseteq W_{ji}.$$

In a similar way, we define the interconnection of estimators $\widehat{\Sigma}_S$ as the following.

Definition 43. *Consider $N \in \mathbb{N}_{\geq 1}$ estimators $\widehat{\Sigma}_{S_i} = (X_i, U_i, W_i, \hat{f}_i, Y_{1_i}, Y_{2_i}, h_{1_i})$, $i \in \{1, \ldots, N\}$, with the input-output configuration similar to (5.4.1)-(5.4.2). The interconnection of $\widehat{\Sigma}_{S_i}$, for any $i \in \{1, \ldots N\}$, is the interconnected estimator $\widehat{\Sigma}_S = (X, U, \hat{f}, Y)$, denoted by $\mathcal{I}(\widehat{\Sigma}_{S_1}, \ldots, \widehat{\Sigma}_{S_N})$, such that $X := \prod_{i=1}^{N} X_i$, $U := \prod_{i=1}^{N} U_i$, $\hat{f} := \prod_{i=1}^{N} \hat{f}_i$, and $Y := \prod_{i=1}^{N} Y_i$, subject to the following constraint:*

$$\forall i, j \in \{1, \ldots, N\}, i \neq j: \quad \hat{w}_{ji} = \hat{y}_{1_{ij}}, \quad Y_{1_{ij}} \subseteq W_{ji}.$$

An example of the interconnection of two POMDPs Σ_{S_1} and Σ_{S_2} is illustrated in Figure 5.1.

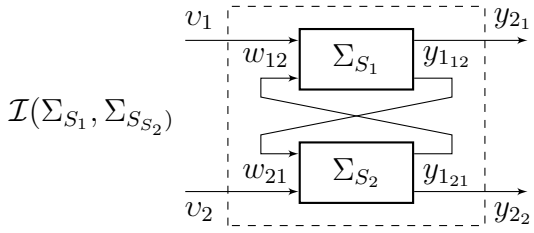

Figure 5.1: Interconnection of two POMDPs Σ_{S_1} and Σ_{S_2}.

5.5 Compositional Construction of CBF

In this section, we analyze networks of POMDP and provide a compositional approach to construct a CBF of an interconnected POMDP based on LCBF of its subsystems. For $i \in \{1, \ldots, N\}$, consider the PO-dt-SCS Σ_{S_i} in (2.3.5), its corresponding estimator $\widehat{\Sigma}_{S_i}$ in (5.2.1), and the augmented system $\widetilde{\Sigma}_S$ in (5.3.1). Assume there exists a LCBF $\mathcal{B}_i$ as defined in Definition 29 or 38 with functions $\alpha_i \in \mathcal{K}_\infty$, $\rho_i \in \mathcal{K}_\infty \cup \{0\}$ and constants $\bar{\beta}_{1_i}, \bar{c}_i \in \mathbb{R}_{\geq 0}$, $\bar{\beta}_{0_i} \in \mathbb{R}_{>0}$, and $0 < \bar{\kappa}_i < 1$. Now we raise the following small-gain assumption that is essential for the compositionality results of this section.

Assumption 5. *Assume that $\mathcal{K}_\infty$ functions $\bar{\kappa}_{ij}$ defined as*

$$\bar{\kappa}_{ij} := \begin{cases} \bar{\kappa}_i, & \text{if } \ i = j, \\ \rho_i \circ \alpha_j^{-1}, & \text{if } \ i \neq j, \end{cases} \quad \forall i, j \in \{1, \ldots, N\},$$

satisfy

$$\bar{\kappa}_{i_1 i_2} \circ \bar{\kappa}_{i_2 i_3} \circ \cdots \circ \bar{\kappa}_{i_{r-1} i_r} \circ \bar{\kappa}_{i_r i_1} < \mathcal{I}_d, \tag{5.5.1}$$

for all sequences $(i_1, \ldots, i_r) \in \{1, \ldots, N\}^r$ and $r \in \{1, \ldots, N\}$.

Remark 44. *The small-gain condition* (5.5.1) *implicitly states that in every strongly connected component of the graph representing the topology of the interconnected system, the effect of strong interconnections can be compensated by weak ones as long as their composition is less than identity.*

Remark 45. *Note that the small-gain condition* (5.5.1) *is a standard one in studying the stability of large-scale interconnected systems via ISS Lyapunov functions [85, 86]. This condition can be readily satisfied if each* $\bar{\kappa}_{ij}$ *is less than identity* ($\bar{\kappa}_{ij} < \mathcal{I}_d, \forall i, j \in \{1, \dots, N\}$). *Since each* $\bar{\kappa}_i$ *is less than identity* ($0 < \bar{\kappa}_i < 1, \forall i \in \{1, \dots, N\}$) *by Definition 29 or 38, one only needs to satisfy* $\rho_i \circ \alpha_j^{-1} < \mathcal{I}_d, \forall i, j \in \{1, \dots, N\}, i \neq j$.

The small-gain condition (5.5.1) implies the existence of $\mathcal{K}_\infty$ functions $\sigma_i > 0$ [87, Theorem 5.5], satisfying

$$\max_{i,j} \left\{ \sigma_i^{-1} \circ \bar{\kappa}_{ij} \circ \sigma_j \right\} < \mathcal{I}_d, \qquad i, j \in \{1, \dots, N\}. \tag{5.5.2}$$

In the next theorem, we show that if Assumption 5 holds and $\max_i \sigma_i^{-1}$ is concave (in order to employ Jensen's inequality), then one can compute a CBF for the interconnected system Σ_S as in Definition 30 in a compositional fashion.

Theorem 46. *Consider the interconnected POMDP* $\Sigma_S = \mathcal{I}(\Sigma_{S_i}, \dots, \Sigma_{S_N})$ *induced by* $N \in \mathbb{N}_{\geq 1}$ *subsystems* Σ_{S_i}. *Suppose that for each* Σ_{S_i} *there exists an estimator* $\widehat{\Sigma}_{S_i}$ *together with a corresponding LCBF* $\mathcal{B}_i$ *as defined in Definition 29 with initial and unsafe sets* X_{0_i} *and* X_{1_i}, *respectively. If Assumption 5 holds and* $\max_i \sigma_i^{-1}$ *for* σ_i *as in* (5.5.2) *is concave and*

$$\max_i \{\sigma_i^{-1}(\bar{\beta}_{0_i})\} < \max_i \{\sigma_i^{-1}(\bar{\beta}_{1_i})\}, \tag{5.5.3}$$

then function $\mathcal{B}(x, \hat{x})$ *defined as*

$$\mathcal{B}(x, \hat{x}) := \max_i \left\{ \sigma_i^{-1}(\mathcal{B}_i(x_i, \hat{x}_i)) \right\}, \tag{5.5.4}$$

is a CBF for the augmented system $\widetilde{\Sigma}_S = [\Sigma_S \ ; \ \widehat{\Sigma}_S]$ *with initial and unsafe sets* $X_0 = \prod_{i=1}^N X_{0_i}$, $X_1 = \prod_{i=1}^N X_{1_i}$, *respectively.*

Proof. We first show that conditions (5.3.6) and (5.3.7) in Definition 30 hold. For any $(x, \hat{x}) \in X_0 \times X_0$, with $X_0 = \prod_{i=1}^N X_{0_i}$, and from (5.3.3), we have

$$\mathcal{B}(x, \hat{x}) = \max_i \left\{ \sigma_i^{-1}(\mathcal{B}_i(x_i, \hat{x}_i)) \right\} \leq \max_i \left\{ \sigma_i^{-1}(\bar{\beta}_{0_i}) \right\} = \beta_0,$$

and simply for any $(x, \hat{x}) \in X_1 \times X$, with $X_1 = \prod_{i=1}^{N} X_{1_i}$, $X = \prod_{i=1}^{N} X_i$ and from (5.3.4), we have

$$\mathcal{B}(x, \hat{x}) = \max_i \left\{\sigma_i^{-1}(\mathcal{B}_i(x_i, \hat{x}_i))\right\} \geq \max_i \left\{\sigma_i^{-1}(\bar{\beta}_{1_i})\right\} = \beta_1,$$

satisfying conditions (5.3.3) and (5.3.4) with $\beta_0 = \max_i \left\{\sigma_i^{-1}(\bar{\beta}_{0_i})\right\}$ and $\beta_1 = \max_i \left\{\sigma_i^{-1}(\bar{\beta}_{1_i})\right\}$. Moreover, $\beta_1 > \beta_0$ according to (5.5.3). Now we show that condition (5.3.8) holds, as well. Let $\kappa(s) = \max_{i,j}\{\sigma_j^{-1} \circ \bar{\kappa}_{ij} \circ \sigma_j(s)\}$. It follows from (5.5.2) that $\kappa < \mathcal{I}_d$. Since $\max_i \sigma_i^{-1}$ is concave, one can readily acquire the chain of inequalities in (5.5.5) using Jensen's inequality. Hence, $\mathcal{B}$ is a CBF for the augmented system $\widetilde{\Sigma}_S = [\Sigma_S; \widehat{\Sigma}_S]$, which completes the proof. □

Remark 47. *Note that inequality* (5.5.3) *in general is not very restrictive. Indeed, functions* σ_i *in* (5.5.2) *play the role of rescaling LCBFs of the individual subsystems while normalizing the effect of internal gains of other subsystems (see [86] for a similar discussion in the context of Lyapunov stability). Due to this scaling, one can expect that such an inequality holds in many applications.*

Remark 48. *The* $\mathcal{K}_\infty$ *functions* $\sigma_i, i \in \{1, \ldots, N\}$*, can always be chosen as identity provided that* $\bar{\kappa}_{ij} < \mathcal{I}_d, \forall i, j \in \{1, \ldots, N\}$*, for functions* $\bar{\kappa}_{ij}$ *defined in Assumption 5.*

Similarly, we propose the next theorem to compute a CBF for an interconnected system Σ_S as in Definition 39 in a compositional way based on LCBFs of subsystems.

Theorem 49. *Consider an interconnected POMDP* $\Sigma_S = \mathcal{I}(\Sigma_{S_i}, \ldots, \Sigma_{S_N})$ *induced by* $N \in \mathbb{N}_{\geq 1}$ *subsystems* Σ_{S_i}*. Suppose that for each* Σ_{S_i} *there exists an estimator* $\widehat{\Sigma}_{S_i}$ *together with a corresponding LCBF* $\mathcal{B}_i$ *as defined in Definition 38 with initial and unsafe sets* X_{0_i} *and* $X_{1_i}^{\epsilon}$*, respectively. If Assumption 5 holds and* $\max_i \sigma_i^{-1}$ *for* σ_i *as in* (5.5.2) *is concave and*

$$\max_i\{\sigma_i^{-1}(\bar{\beta}_{0_i})\} < \max_i\{\sigma_i^{-1}(\bar{\beta}_{1_i})\}, \tag{5.5.6}$$

then function $\mathcal{B}(x)$ *defined as*

$$\mathcal{B}(x) := \max_i \left\{\sigma_i^{-1}(\mathcal{B}_i(x_i))\right\}, \tag{5.5.7}$$

is a CBF for the estimator $\widehat{\Sigma}_S = \mathcal{I}(\widehat{\Sigma}_{S_i}, \ldots, \widehat{\Sigma}_{S_N})$ *with initial and unsafe sets* $X_0 = \prod_{i=1}^{N} X_{0_i}$, $X_1^{\epsilon} = \prod_{i=1}^{N} X_{1_i}^{\epsilon}$*, respectively.*

The proof of Theorem 49 follows the same reasoning as that of Theorem 46 and is therefore omitted.

Remark 50. *In the case of sum-of-squares optimization approach, the computational complexity of finding polynomial-type local barrier functions depends on both the degree of polynomials and the number of state variables. One can easily see that for fixed degrees of*

$$
\begin{aligned}
&\mathbb{E}\Big[\mathcal{B}(f(x(k),\upsilon(k),\varsigma_1(k)),\hat{f}(\hat{x}(k),\upsilon(k),y(k)))\,\big|\,x(k),\hat{x}(k),\upsilon(k)\Big]\\
&\quad=\mathbb{E}\Big[\max_i\Big\{\sigma_i^{-1}(\mathcal{B}_i(f_i(x_i(k),\upsilon_i(k),w_i(k),\varsigma_{1_i}(k)),\hat{f}_i(\hat{x}_i(k),\upsilon_i(k),\hat{w}_i(k),y_{2_i}(k))))\Big\}\\
&\quad\big|\,x(k),\hat{x}(k),\upsilon(k),w(k),\hat{w}(k)\Big]\\
&\quad\le\max_i\Big\{\sigma_i^{-1}(\mathbb{E}\Big[\mathcal{B}_i(f_i(x_i(k),\upsilon_i(k),w_i(k),\varsigma_{1_i}(k)),\hat{f}_i(\hat{x}_i(k),\upsilon_i(k),\hat{w}_i(k),y_{2_i}(k)))\\
&\quad\big|\,x(k),\hat{x}(k),\upsilon(k),w(k),\hat{w}(k)\Big])\Big\}\\
&\quad=\max_i\Big\{\sigma_i^{-1}(\mathbb{E}\Big[\mathcal{B}_i(f_i(x_i(k),\upsilon_i(k),w_i(k),\varsigma_{1_i}(k)),\hat{f}_i(\hat{x}_i(k),\upsilon_i(k),\hat{w}_i(k),y_{2_i}(k)))\\
&\quad\big|\,x_i(k),\hat{x}_i(k),\upsilon_i(k),w_i(k),\hat{w}_i(k)\Big])\Big\}\\
&\quad\le\max_i\Big\{\sigma_i^{-1}(\max\{\bar{\kappa}_i(\mathcal{B}_i(x_i(k),\hat{x}_i(k))),\rho_i(\|\begin{bmatrix}w_i(k)\\\hat{w}_i(k)\end{bmatrix}\|^2),\bar{c}_i\})\Big\}\\
&\quad=\max_i\Big\{\sigma_i^{-1}(\max\{\bar{\kappa}_i(\mathcal{B}_i(x_i(k),\hat{x}_i(k))),\rho_i(\max_{j,j\neq i}\|\begin{bmatrix}w_{ij}(k)\\\hat{w}_{ij}(k)\end{bmatrix}\|^2),\bar{c}_i\})\Big\}\\
&\quad=\max_i\Big\{\sigma_i^{-1}(\max\{\bar{\kappa}_i(\mathcal{B}_i(x_i(k),\hat{x}_i(k))),\rho_i(\max_{j,j\neq i}\|\begin{bmatrix}y_{1_{ji}}(k)\\\hat{y}_{1_{ji}}(k)\end{bmatrix}\|^2),\bar{c}_i\})\Big\}\\
&\quad\le\max_i\Big\{\sigma_i^{-1}(\max\{\bar{\kappa}_i(\mathcal{B}_i(x_i(k),\hat{x}_i(k))),\rho_i(\max_{j,j\neq i}\|\begin{bmatrix}h_{1_j}(x_j(k))\\h_{1_j}(\hat{x}_j(k))\end{bmatrix}\|^2),\bar{c}_i\})\Big\}\\
&\quad\le\max_i\Big\{\sigma_i^{-1}(\max\{\bar{\kappa}_i(\mathcal{B}_i(x_i(k),\hat{x}_i(k))),\rho_i(\max_{j,j\neq i}\{\alpha_j^{-1}(\mathcal{B}_j(x_j(k),\hat{x}_j(k)))\}),\bar{c}_i\})\Big\}\\
&\quad=\max_{i,j}\Big\{\sigma_i^{-1}(\max\{\bar{\kappa}_{ij}(\mathcal{B}_i(x_i(k),\hat{x}_i(k))),\bar{c}_i\})\Big\}\\
&\quad=\max_{i,j}\Big\{\sigma_i^{-1}(\max\{\bar{\kappa}_{ij}\circ\sigma_j\circ\sigma_j^{-1}(\mathcal{B}_j(x_j(k),\hat{x}_j(k))),\bar{c}_i\})\Big\}\\
&\quad\le\max_{i,j,l}\Big\{\sigma_i^{-1}(\max\{\bar{\kappa}_{ij}\circ\sigma_j\circ\sigma_l^{-1}(\mathcal{B}_l(x_l(k),\hat{x}_l(k))),\bar{c}_i\})\Big\}\\
&\quad=\max_{i,j}\Big\{\sigma_i^{-1}(\max\{\bar{\kappa}_{ij}\circ\sigma_j(\mathcal{B}(x(k),\hat{x}(k))),\bar{c}_i\})\Big\}=\max\{\kappa(\mathcal{B}(x(k),\hat{x}(k))),c\Big\}.
\end{aligned}
\tag{5.5.5}
$$

polynomials, the required computations grow polynomially with respect to the dimension of the (augmented) subsystems [45]. Furthermore, the computational complexity of finding a CBF for the interconnected system is linear with respect to the number of subsystems. In the counter example guided inductive synthesis (CEGIS) approach proposed in [14, Section 5.1], due to its iterative nature and lack of guarantee on the termination, it is difficult to provide any analysis on the computational complexity with respect to the dimension of subsystems. Evidently in both SOS and CEGIS approach, the computational complexity is independent of the time horizon T_d.

Finally, we provide an approach to compositionally construct an SSF for an interconnected POMDP Σ_S based on SPSFs of its subsystems. Note that the constructed SSF is one of the main ingredients used in Theorem 40. First, we raise the following small-gain assumption.

Assumption 6. *Assume that $\mathcal{K}_\infty$ functions $\bar{c}_{2ij}$ defined as*

$$\bar{c}_{2ij} := \begin{cases} \bar{c}_{2i}, & \text{if } i = j, \\ \varrho_i \circ \varepsilon_j^{-1}, & \text{if } i \neq j, \end{cases} \quad \forall i, j \in \{1, \dots, N\},$$

satisfy

$$\bar{c}_{2i_1 i_2} \circ \bar{c}_{2i_2 i_3} \circ \cdots \circ \bar{c}_{2i_{r-1} i_r} \circ \bar{c}_{2i_r i_1} < \mathcal{I}_d, \tag{5.5.8}$$

for all sequences $(i_1, \dots, i_r) \in \{1, \dots, N\}^r$ and $r \in \{1, \dots, N\}$.

The small-gain condition (5.5.8) implies the existence of $\mathcal{K}_\infty$ functions $\zeta_i > 0$ [87, Theorem 5.5], satisfying

$$\max_{i,j} \left\{ \zeta_i^{-1} \circ \bar{c}_{2ij} \circ \zeta_j \right\} < \mathcal{I}_d, \qquad i, j = \{1, \dots, N\}. \tag{5.5.9}$$

In the next proposition, we show that if Assumption 6 holds and $\max_i \zeta_i^{-1}$ is concave, then we can compositionally construct an SSF for an interconnected system based on SPSFs of its subsystems.

Proposition 51. *Consider an interconnected POMDP $\Sigma_S = \mathcal{I}(\Sigma_{S_i}, \dots, \Sigma_{S_N})$ induced by $N \in \mathbb{N}_{\geq 1}$ subsystems Σ_{S_i}. Suppose that for each Σ_{S_i} there exists an estimator $\widehat{\Sigma}_{S_i}$ together with a corresponding SPSF $\boldsymbol{\phi}_i(x_i, \hat{x}_i)$. If Assumption 6 holds and $\max_i \zeta_i^{-1}$ for ζ_i as in (5.5.9) is concave, then the function $\boldsymbol{\phi}(x, \hat{x})$ defined as*

$$\boldsymbol{\phi}(x, \hat{x}) := \max_i \left\{ \zeta_i^{-1}(\boldsymbol{\phi}_i(x_i, \hat{x}_i)) \right\},$$

is an SSF from $\widehat{\Sigma}_S = \mathcal{I}(\widehat{\Sigma}_{S_i}, \dots, \widehat{\Sigma}_{S_N})$ to $\Sigma_S = \mathcal{I}(\Sigma_{S_i}, \dots, \Sigma_{S_N})$, as defined in Definition 36, with

$$\begin{aligned} c_2(s) &= \max_{i,j} \left\{ \zeta_i^{-1} \circ \bar{c}_{2ij} \circ \zeta_j(s) \right\}, \quad i, j = \{1, \dots, N\}, \\ c_1 &= \max_i \zeta_i^{-1}(\bar{c}_{1_i}). \end{aligned}$$

The proof of Proposition 51 follows the same reasoning as that of Theorem 46 and is omitted here.

5.6 Computation of LCBF

In this section, we provide a systematic approach to search for LCBFs and the corresponding control policies for subsystems. The proposed approach is based on the sum-of-squares (SOS) optimization problem [88], in which LCBF is restricted to be non-negative which can be written as a sum of squares of different polynomials. To do so, we need to raise the following assumption.

Assumption 7. *For the POMDP $\Sigma_S = (X, U, W, \varsigma_1, f, Y_1, Y_2, h_1, h_2, \varsigma_2)$, the transition map $f : X \times U \times W \times V_{\varsigma_1} \to X$ is a polynomial function of its arguments. Furthermore, the internal output map $h_1 : X \to Y_1$ and $\mathcal{K}_\infty$ functions α and ρ are polynomial.*

Under Assumption 7, one can reformulate conditions of Definition 29 and Definition 38 to an SOS optimization problem in order to search for a polynomial LCBF $\mathcal{B}_i(\cdot,\cdot)$ and $\mathcal{B}_i(\cdot)$, and their corresponding control policies. In the following Lemmas, SOS formulations are provided.

Lemma 52. *Suppose Assumption 7 holds and sets X_0, X_1, X, W can be defined by vectors of polynomial inequalities $X_0 = \{x \in \mathbb{R}^n \mid g_a(x) \geq 0\}, X_1 = \{x \in \mathbb{R}^n \mid g_b(x) \geq 0\}, X = \{x \in \mathbb{R}^n \mid \tilde{g}(x) \geq 0\}$, $W = \{w \in \mathbb{R}^p \mid g_w(w) \geq 0\}$, and $U = \{\upsilon(k) \in \mathbb{R}^m \mid g_c(\upsilon(k)) \geq 0\}$, where the inequalities are defined element-wise. Suppose there exists a sum-of-square polynomial $\mathcal{B}(x, \hat{x})$, constants $\bar{\beta}_0, \tilde{c} \in \mathbb{R}_{\geq 0}, \bar{\beta}_1 \in \mathbb{R}_{>0}$, $0 < \tilde{\kappa} < 1$, functions $\alpha \in \mathcal{K}_\infty, \tilde{\rho} \in \mathcal{K}_\infty \cup \{0\}$, polynomials $l_{\upsilon_j}(\hat{x}, \hat{w})$ corresponding to the j^{th} input in $\upsilon(k) = (\upsilon_1(k), \upsilon_2(k), \ldots, \upsilon_m(k)) \in U \subseteq \mathbb{R}^m$, and vectors of sum-of-squares polynomials $l_z(x), \hat{l}_z(\hat{x})$ for $z \in \{0, 1, 2, 3\}$, and $l_c(\upsilon(k)), l_w(w), \hat{l}_w(\hat{w})$, of appropriate dimensions such that the following expressions are sum-of-square polynomials:*

$$\mathcal{B}(x,\hat{x}) - \begin{bmatrix} l_0^\top(x) & \hat{l}_0^\top(\hat{x}) \end{bmatrix} \begin{bmatrix} \tilde{g}(x) \\ \tilde{g}(\hat{x}) \end{bmatrix} - \alpha\Big(\begin{bmatrix} h_1(x) \\ h_1(\hat{x}) \end{bmatrix}^\top \begin{bmatrix} h_1(x) \\ h_1(\hat{x}) \end{bmatrix} \Big), \tag{5.6.1}$$

$$-\mathcal{B}(x,\hat{x}) - \begin{bmatrix} l_1^\top(x) & \hat{l}_1^\top(\hat{x}) \end{bmatrix} \begin{bmatrix} g_a(x) \\ g_a(\hat{x}) \end{bmatrix} + \bar{\beta}_1, \tag{5.6.2}$$

$$\mathcal{B}(x,\hat{x}) - \begin{bmatrix} l_2^\top(x) & \hat{l}_2^\top(\hat{x}) \end{bmatrix} \begin{bmatrix} g_b(x) \\ \tilde{g}(\hat{x}) \end{bmatrix} + \bar{\beta}_0, \tag{5.6.3}$$

$$\begin{aligned} -\mathbb{E}\Big[\mathcal{B}\big(f(x(k), \upsilon(k), w(k), \varsigma_1(k)), \hat{f}(\hat{x}(k), \upsilon(k), \hat{w}(k), y_2(k))\big), \,\Big|\, x(k), \hat{x}(k), \upsilon(k), w(k), \hat{w}(k) \Big] \\ + \tilde{\kappa}\mathcal{B}(x(k), \hat{x}(k)) + \tilde{\rho}\Big(\frac{\begin{bmatrix} w(k) \\ \hat{w}(k) \end{bmatrix}^\top \begin{bmatrix} w(k) \\ \hat{w}(k) \end{bmatrix}}{2p} \Big) + \tilde{c} - \sum_{j=1}^{m} (\upsilon_j(k) - l_{\upsilon_j}(\hat{x}(k), \hat{w}(k))) \\ - \begin{bmatrix} l_3^\top(x(k)) & \hat{l}_3^\top(\hat{x}(k)) \end{bmatrix} \begin{bmatrix} \tilde{g}(x(k)) \\ \tilde{g}(\hat{x}(k)) \end{bmatrix} - \begin{bmatrix} l_w^\top(w(k)) & \hat{l}_w^\top(\hat{w}(k)) \end{bmatrix} \begin{bmatrix} g_w(w(k)) \\ g_w(\hat{w}(k)) \end{bmatrix} - l_c^\top(\upsilon(k)) g_c(\upsilon(k)), \end{aligned} \tag{5.6.4}$$

where p is the dimension of the internal inputs w and $\hat{w}$. Then $\mathcal{B}(x,\hat{x})$ satisfies conditions (5.3.2)-(5.3.17) *in Definition 29 and $\upsilon(k) = [l_{\upsilon_1}(\hat{x}(k),\hat{w}(k)); \ldots; l_{\upsilon_m}(\hat{x}(k)\hat{w}(k))]$ is the corresponding safety controller, with*

$$\begin{aligned}
\bar{\kappa} =& \mathcal{I}_d - (\mathcal{I}_d - \pi_1) \circ (\mathcal{I}_d - \tilde{\kappa}),\\
\rho =& (\mathcal{I}_d + \pi_2) \circ (\mathcal{I}_d - \tilde{\kappa})^{-1} \circ \pi_1^{-1} \circ \pi_3 \circ \tilde{\rho},\\
\bar{c} =& (\mathcal{I}_d + \pi_2^{-1}) \circ (\mathcal{I}_d - \tilde{\kappa})^{-1} \circ \pi_1^{-1} \circ \pi_3 \circ (\pi_3 - \mathcal{I}_d)^{-1} \circ (\tilde{c}),
\end{aligned}$$

where π_1, π_2, π_3 being some arbitrarily chosen $\mathcal{K}_\infty$ functions so that $(\mathcal{I}_d - \pi_1) \in \mathcal{K}_\infty$, and $(\pi_3 - \mathcal{I}_d) \in \mathcal{K}_\infty$.

The proof follows the same argument as in [14, Lemma 5.9], and is therefore omitted.

Remark 53. *Inequalities* (5.3.2) *and* (5.3.5) *consider infinity norms over $\left[h_1(x); h_1(\hat{x})\right]$ and $\left[w; \hat{w}\right]$, respectively. Since such norms cannot be expressed as polynomials, we convert infinity norms to Euclidean ones and that is the reason constant $2p$ appears as a denominator in* (5.6.4).

Remark 54. *Note that even if the functions mentioned in Assumption 7 are not polynomials, one can still use the proposed results in the chapter by searching for LCBFs via CEGIS (we refer interested readers to [14, Section 5.1] for more details on the CEGIS framework).*

We now state another lemma for the computation of LCBF as in Definition 38.

Lemma 55. *Suppose Assumption 7 holds and sets $X_0, X_1^\epsilon, X, W, Y_2$ can be defined by vectors of polynomial inequalities $X_0 = \{x \in \mathbb{R}^n \mid g_a(x) \geq 0\}, X_1^\epsilon = \{x \in \mathbb{R}^n \mid g_b^\epsilon(x) \geq 0\}, X = \{x \in \mathbb{R}^n \mid \tilde{g}(x) \geq 0\}$, $U = \{\upsilon(k) \in \mathbb{R}^m \mid g_c(\upsilon(k)) \geq 0\}$, and $W = \{w \in \mathbb{R}^p \mid g_w(w) \geq 0\}$, where the inequalities are defined element-wise. Suppose there exists a sum-of-square polynomial $\mathcal{B}(x)$, constants $\bar{\beta}_0, \tilde{c} \in \mathbb{R}_{\geq 0}, \bar{\beta}_1 \in \mathbb{R}_{>0}$, $0 < \tilde{\kappa} < 1$, functions $\alpha, \varkappa \in \mathcal{K}_\infty, \tilde{\rho} \in \mathcal{K}_\infty \cup \{0\}$, polynomials $l_{\upsilon_j}(\hat{x},\hat{w})$ corresponding to the j^{th} input in $\upsilon(k) = (\upsilon_1(k), \upsilon_2(k), \ldots, \upsilon_m(k)) \in U \subseteq \mathbb{R}^m$, and vectors of sum-of-squares polynomials $l_z(x)$ for $z \in \{0,1,2,3\}$, $\hat{l}_3(\hat{x})$, $l_c(\upsilon(k))$, and $\hat{l}_w(\hat{w})$ of appropriate dimensions such that the following expressions are sum-of-square polynomials:*

$$\mathcal{B}(x) - l_0^\top(x)\tilde{g}(x) - \alpha(h_1(x)^\top h_1(x)), \tag{5.6.5}$$

$$-\mathcal{B}(x) - l_1^\top(x) g_a(x) + \bar{\beta}_1, \tag{5.6.6}$$

$$\mathcal{B}(x) - l_2^\top(x) g_b^\epsilon(x) + \bar{\beta}_0, \tag{5.6.7}$$

$$
\begin{aligned}
&-\mathbb{E}\Big[\mathcal{B}\big(\hat{f}(\hat{x}(k),\upsilon(k),\hat{w}(k),h_2(x(k),\varsigma_2(k)))\big)\,|\,\hat{x}(k),\upsilon(k),\hat{w}(k),x(k)\Big]+\tilde{\kappa}\mathcal{B}(\hat{x}(k))\\
&\quad+\tilde{\rho}(\frac{\hat{w}^\top(k)\hat{w}(k)}{p})+\tilde{c}+\varkappa(\frac{(x(k)-\hat{x}(k))^\top(x(k)-\hat{x}(k))}{n})\\
&\quad-\sum_{j=1}^{m}(\upsilon_j(k)-l_{\upsilon_j}(\hat{x}(k),\hat{w}(k)))-l_3^\top(x(k))\tilde{g}(x(k))-\hat{l}_3^\top(\hat{x}(k))\tilde{g}(\hat{x}(k))\\
&\quad-\hat{l}_w^\top(\hat{w}(k))g_w(\hat{w}(k))\ -l_c^\top(\upsilon(k))g_c(\upsilon(k)),
\end{aligned}
\tag{5.6.8}
$$

where p and n are the dimensions of the internal input w and state x, respectively. Then $\mathcal{B}(\hat{x})$ satisfies conditions (5.3.14)-(5.3.17) *in Definition 38 and*

$$\upsilon(k)=[l_{\upsilon_1}(\hat{x}(k),\hat{w}(k));\ldots;l_{\upsilon_m}(\hat{x}(k),\hat{w}(k))],$$

is the corresponding safety controller, where $\bar{\kappa},\rho,\bar{c}$ can be acquired based on $\tilde{\kappa},\tilde{\rho},\tilde{c}$ similar to Lemma 52.

Remark 56. *In order to compute the sum-of-square polynomials $\mathcal{B}(x,\hat{x})$ and $\mathcal{B}(x)$ fulfilling reformulated conditions* (5.6.1)-(5.6.4)*, and* (5.6.5)-(5.6.8)*, one can employ existing software tools such as SOSTOOLS [63] together with a semidefinite programming solver such as SeDuMi [64].*

5.7 Case Study

In this section, we illustrate our proposed results by applying them to an adaptive cruise control (ACC) system consisting of N vehicles in a platoon (see Figure 5.2). This model is adapted from [89]. The evolution of states can be described by the interconnected PO-dt-SCS

$$\Sigma_S:\begin{cases}x(k+1)=\bar{A}x(k)+\bar{B}\upsilon(k)+\varsigma_1(k),\\ y(k)=\bar{C}x(k)+\varsigma_2(k),\end{cases}$$

where $\bar{A}$ is a block matrix with diagonal blocks A, and off-diagonal blocks $A_{i(i-1)}=A_w, i\in\{2,\ldots,N\}$, where

$$A=\begin{bmatrix}1&-1\\0&1\end{bmatrix},\quad A_w=\begin{bmatrix}0&\tau\\0&0\end{bmatrix},$$

with $\tau=0.01$ being the interconnection degree, and all other off-diagonal blocks being zero matrices of appropriate dimensions. Moreover, $\bar{B}$ is a partitioned matrix with main diagonal blocks $B=[0\,;1]$, and all other off-diagonal blocks being zero matrices of appropriate dimensions. The matrix $\bar{C}$ is a partitioned matrix with main diagonal blocks $C=[1\,;0]^\top$ and all other off-diagonal blocks being zero matrices of appropriate dimensions. Moreover, $x(k)=[x_1(k);\ldots;x_N(k)]$, $\upsilon(k)=[\upsilon_1(k);\ldots;\upsilon_N(k)]$, $\varsigma_1(k)=[\varsigma_{1_1}(k);\ldots;\varsigma_{1_N}(k)]$, and

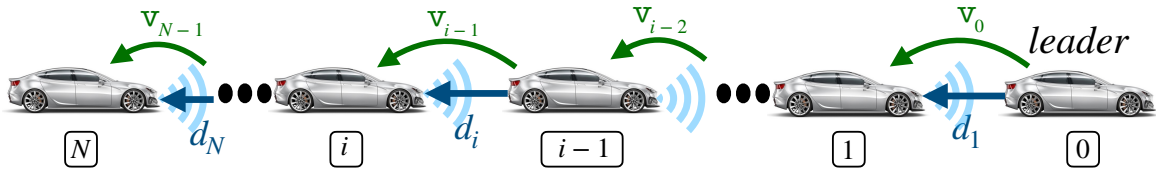

Figure 5.2: Platoon model for $N = 1000$ vehicles.

$\varsigma_2(k) = [\varsigma_{2_1}(k); \ldots; \varsigma_{2_N}(k)]$, where $\varsigma_1(k), \varsigma_2(k)$ have standard normal distributions. Let us consider each individual vehicle Σ_{S_i} described as

$$\Sigma_{S_i} : \begin{cases} x_i(k+1) = Ax_i(k) + B\upsilon_i(k) + A_w w_i(k) + \varsigma_{1_i}(k), \\ y_{1_i}(k) = C_1 x_i(k), \\ y_{2_i}(k) = C_2 x_i(k) + \varsigma_{2_i}(k), \end{cases}$$

where $y_{1_i}(k) = y_{1_{i(i+1)}}(k) = C_1 x_i(k), i \in \{1, \ldots N\}$, (with $C_1 = [0\,;1]$ and $y_{1_{N(N+1)}} = 0$) and $C_2 = C$. One can readily verify that $\Sigma_S = \mathcal{I}(\Sigma_{S_i}, \ldots, \Sigma_{S_N})$, where $w_i(k) = [0; w_{i(i-1)}(k)], i \in \{1, \ldots, N\}$, (with $w_{i(i-1)} = y_{1_{(i-1)i}} = C_1 x_{i-1}, w_{1,0} = 0$). The state of the i-th vehicle is defined as $x_i = [d_i; \mathrm{v}_i]$, for $i \in \{1, \ldots, N\}$, where d_i denotes the relative distance between the vehicle i and its proceeding vehicle $i-1$ (the 0-*th* vehicle represents the leader), v_i is its velocity in the leader's frame, and $\upsilon_i \in [-1, 1]$ is the bounded control input. The overall control objective in ACC is for each vehicle to adjust its speed in order to maintain a safe distance from the vehicle ahead [90]. For the system Σ_{S_i}, we design a proper estimator of the following form

$$\hat{\Sigma}_{S_i} : \begin{cases} \hat{x}_i(k+1) = A\hat{x}_i(k) + B\upsilon_i(k) + A_w\hat{w}_i(k) \\ \qquad\qquad + K(y_{2_i}(k) - C_2\hat{x}_i(k)), \\ \hat{y}_{1_i}(k) = C_1\hat{x}_i(k), \end{cases}$$

where $K = [1.7; -0.72]$ is the estimator gain. We consider a network of $N = 1000$ vehicles where the regions of interest for each vehicle are $X \in [0, 3.5] \times [-2, 3]$, $X_0 \in [1, 1.5] \times [-0.4, 0.4]$, and $X_1 \in [0, 0.5] \times [-2, -1.5] \cup [3, 3.5] \times [2.5, 3]$. Now, for each vehicle we compute LCBFs while compositionally synthesizing safety controllers for a bounded-time horizon. We construct LCBFs using the two methods introduced in Section 5.3 and employ the software SOSTOOLS to search for LCBFs as described in Section 5.6. According to Section 5.3.1, we compute the LCBF $\mathcal{B}_i(x_i, \hat{x}_i)$ of an order 4 and its corresponding controller as the following:

$$\upsilon_i(\hat{d}_i, \hat{\mathrm{v}}_i, \hat{\mathrm{v}}_{i-1}) = 0.06\hat{d}_i - 0.72\hat{\mathrm{v}}_i - 0.01\hat{\mathrm{v}}_{i-1} - 0.08, \tag{5.7.1}$$

for $i \in \{1, \ldots, N\}$, with a computation time of about 9 minutes. Moreover, the corresponding constants and functions in Definition 29 are quantified as $\alpha_i(s) = 10^{-5}s, s \in \mathbb{R}_{\geq 0}, \bar{\beta}_{0_i} = 0.1, \bar{\beta}_{1_i} = 2, \bar{\kappa}_i = 0.95, \rho_i(s) = 2 \times 10^{-8}s, s \in \mathbb{R}_{\geq 0}, \bar{c}_i = 0.001$. Now, we check the small gain condition (5.5.1) that is required for the compositionality result. By taking $\sigma_i(s) = s$, $i \in \{1, \ldots, N\}$, the condition (5.5.1), and as a result the condition

(5.5.2) are always satisfied without any restriction on the number of vehicles. Hence, $\mathcal{B}(x,\hat{x}) = \max_i \mathcal{B}_i(x_i,\hat{x}_i)$ is a CBF for Σ_S satisfying conditions in Definition 30 with $\beta_0 = 0.1, \beta_1 = 2, \kappa = 0.95$, and $c = 0.001$. By employing Theorem 33, one can guarantee that states of the interconnected system starting from X_0 remain in the safe set $X \backslash X_1$ within the time horizon $T_d = 60$ with a probability of at least 92.19% (*i.e.,* $1-\delta = 0.9219$). Closed-loop state and input trajectories of a representative vehicle with different noise realizations are illustrated in Figure 5.3 with only 10 trajectories.

We now construct the LCBF $\mathcal{B}_i(\hat{x}_i)$ of an order 4 for the estimator, as described in Section 5.3.2, and compute its corresponding controller as

$$\mathsf{u}_i(\hat{d}_i, \hat{\mathrm{v}}_i, \hat{\mathrm{v}}_{i-1}) = 0.08\hat{d}_i - 0.9\hat{\mathrm{v}}_i + 0.02\hat{\mathrm{v}}_{i-1} - 0.1, \tag{5.7.2}$$

for $i \in \{1,\dots,N\}$ with a computation time of about 2 minutes. The corresponding constants and functions in Definition 38 are quantified as $\alpha_i(s) = 10^{-5}s, s \in \mathbb{R}_{\geq 0}$,$\bar{\beta}_{0_i} = 0.1$, $\bar{\beta}_{1_i} = 2, \bar{\kappa}_i = 0.95, \rho_i(s) = 2 \times 10^{-8}s, s \in \mathbb{R}_{\geq 0}, \bar{c}_i = 0.001$, and $\varkappa_i(s) = 10^{-6}s, s \in \mathbb{R}_{\geq 0}$. Similar to the first method, we check the small gain condition (5.5.1) for the compositionality result. By taking $\sigma_i(s) = s$, $i \in \{1,\dots,N\}$, the condition (5.5.1), and as a result the condition (5.5.2) are both satisfied. Hence, $\mathcal{B}(\hat{x}) = \max_i \mathcal{B}_i(\hat{x}_i)$ is a CBF for Σ_S satisfying conditions in Definition 39 with $\beta_0 = 0.1, \beta_1 = 2$, $\kappa = 0.95, c = 0.001$, and $\varkappa(s) = 10^{-6}s, s \in \mathbb{R}_{\geq 0}$. By employing the result of Theorem 33, one can guarantee that the states of the estimator, with accuracy $\epsilon = 0.01$, starting from X_0 will not reach X_1^ϵ within the time horizon $T_d = 60$ with a probability of at least 92.19% (*i.e.,* $1-\delta = 0.9219$). Now, in order to compute the exit probability bound for the interconnected system, we search for an SPSF of a quadratic form $\boldsymbol{\phi}_i(x_i,\hat{x}_i) = (x_i - \hat{x}_i)^\top M (x_i - \hat{x}_i)$, where M is a positive-definite matrix. Since the dynamic of the system is linear, the conditions in Definition 35 reduce to solving the following matrix inequality:

$$(1 + 2/\tilde{\pi})(A - KC_2)^\top M (A - KC_2) \leq \bar{c}_2 M,$$

where K is the estimator gain, and $\tilde{\pi} > 0$. By using the tool YALMIP [40], we compute M as

$$M = \begin{bmatrix} 0.0257 & 0.0259 \\ 0.0259 & 0.0262 \end{bmatrix},$$

with $\tilde{\pi} = 1$. The functions and constants associated with this SPSF are computed by following the compositional construction method for linear systems introduced in [68, Theorem 6.10] as $\varepsilon(s) = 0.3s^2, s \in \mathbb{R}_{\geq 0}, \bar{c}_2 = 0.4, \varrho(s) = 0.002s^2, s \in \mathbb{R}_{\geq 0}, \bar{c}_1 = 10^{-6}$. Hence, $\boldsymbol{\phi}(x,\hat{x}) = \max_i \boldsymbol{\phi}_i(x_i,\hat{x}_i)$ is an SSF from $\widehat{\Sigma}_S$ to Σ_S satisfying the conditions in Definition 36 with $\varepsilon(s) = 0.3s^2, s \in \mathbb{R}_{\geq 0}, c_2 = 0.4$, $c_1 = 10^{-6}$ and $\epsilon = 0.01$. An upper bound of 2.31% (*i.e.,* $\theta = 0.0231$) on the probability of the estimation accuracy is computed according to Theorem 37 within the time horizon $T_d = 60$. Employing Theorem 40, the probability that the solution process of the system starting from the initial region X_0 and not reaching X_1 is at least 90.06% (*i.e.,* $(1-\delta)(1-\theta) = 0.9006$) . Closed-loop state and input trajectories of a representative vehicle with different noise realizations are illustrated in Figure 5.4.

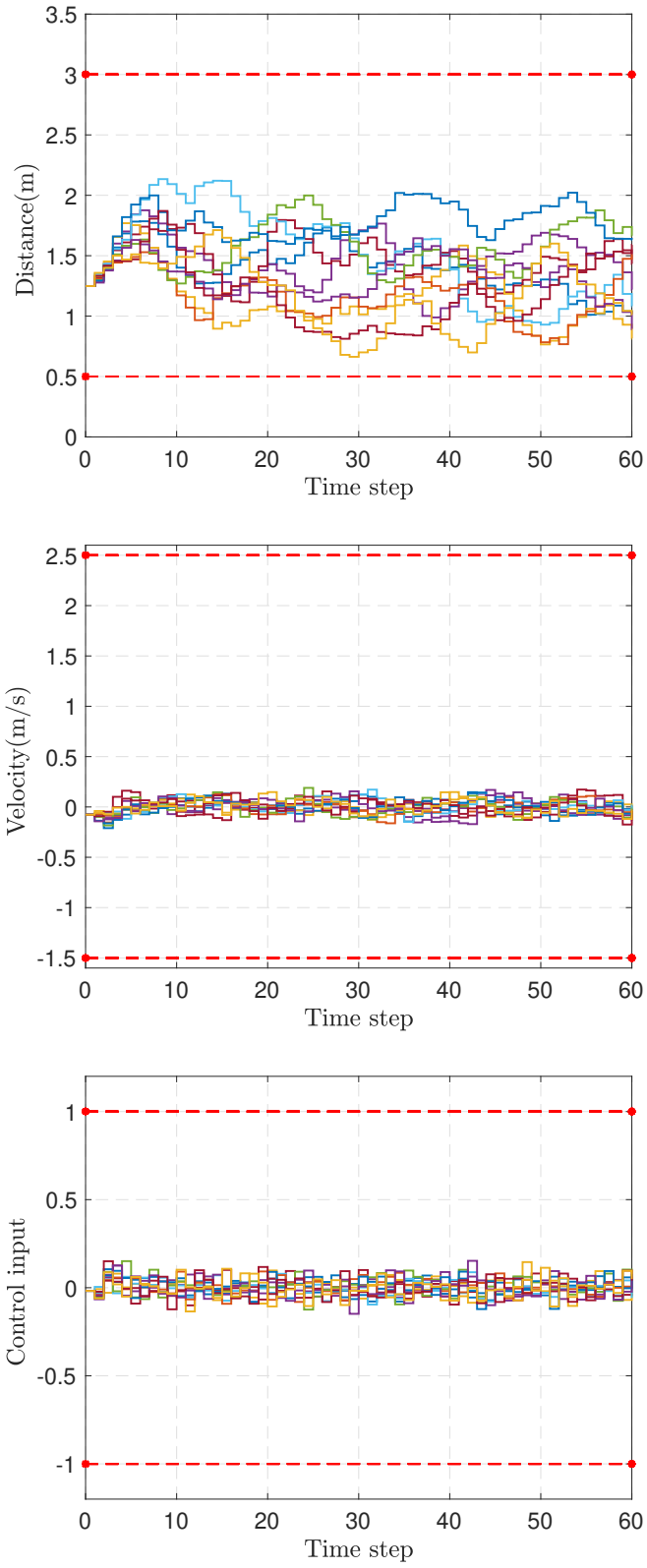

Figure 5.3: Closed-loop state (distance and velocity) and input trajectories of a representative vehicle with different noise realizations in a network of 1000 vehicles under controller (5.7.1).

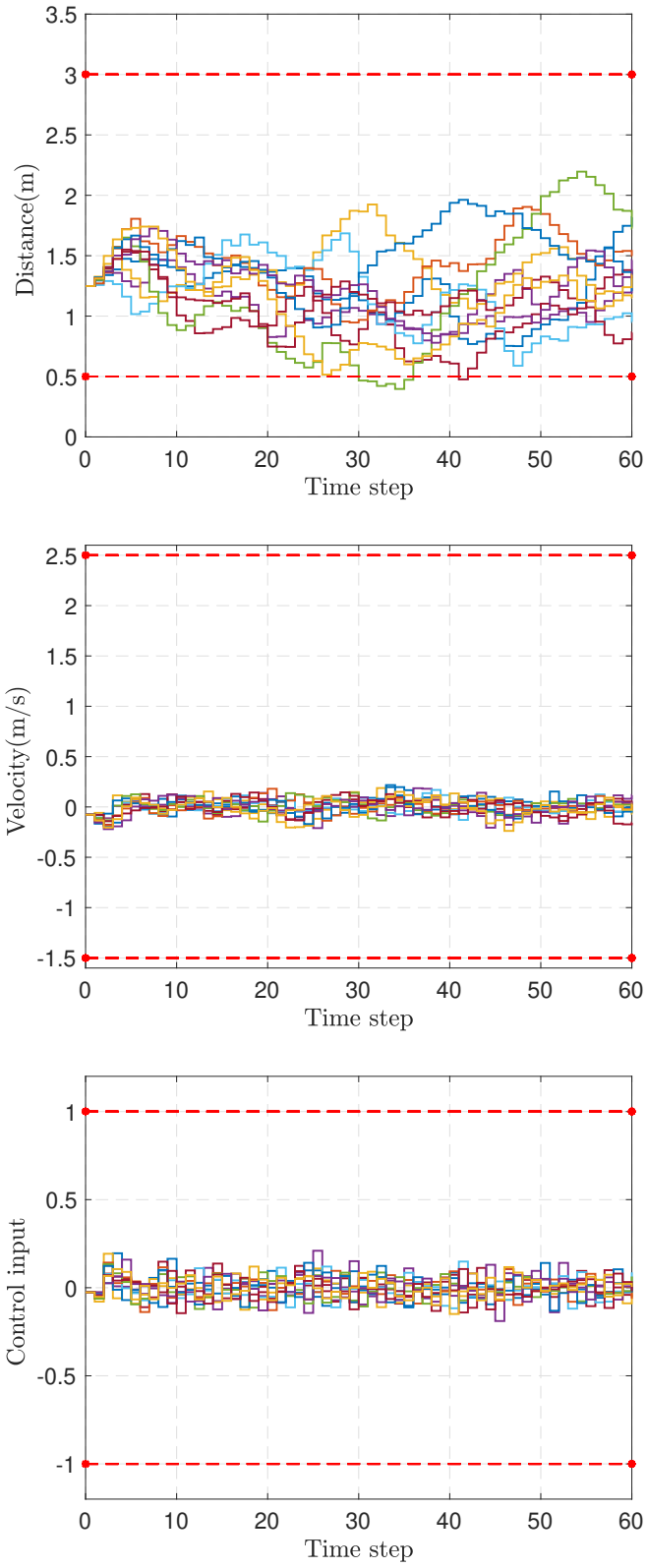

Figure 5.4: Closed-loop state (distance and velocity) and input trajectories of a representative vehicle with different noise realizations in a network of 1000 vehicles under controller (5.7.2).

5.8 Summary

In this chapter, we proposed a compositional approach based on control barrier functions for the synthesis of safety controllers for networks of POMDP by utilizing small-gain type reasoning. The proposed scheme provides an upper bound on the probability that the interconnected system reaches an unsafe region in a finite time horizon. In this respect, we first quantified probability bounds without any prior information on the estimation accuracy. This is achieved by constructing local barrier functions over an augmented system composed of subsystems and their corresponding estimators. Alternatively, we formulated local barrier functions based on only estimators' dynamics and computed the exit probability by utilizing the probability bound on the estimation accuracy computed via notions of stochastic simulation functions. We finally demonstrated the effectiveness of our proposed results by applying them to an adaptive cruise control problem.

Chapter 6

Synthesis of Controllers for Partially-Observable Systems: A Data-Driven Approach

This chapter is concerned with the formal synthesis of safety controllers for partially-observable continuous-time polynomial-type systems with unknown dynamics. Given a continuous-time polynomial-type estimator with a *partially-unknown* dynamic and a *known* upper bound on the estimation accuracy, we propose a data-driven approach to compute a polynomial-type controller ensuring the safety of the system. The proposed framework is based on a notion of so-called *control barrier functions* and only requires a single output trajectory collected from the system and a single state trajectory collected from its estimator. We show the application of our technique by synthesizing a safety controller for a partially-observable jet engine with unknown dynamics.

6.1 Introduction

The conventional methods to synthesize controllers, including the ones proposed in the previous chapters, require precise models of dynamical systems. However, closed-form mathematical models of many physical systems are either unavailable or too complicated to be of any use. Therefore, it is not possible to analyze or synthesize controllers for complex systems with unknown models using model-based methodologies. Since obtaining precise models for complex systems is typically a tedious and costly task [91], data-driven approaches are becoming increasingly popular when dealing with systems with unknown dynamics.

6.1.1 Related Literature

Over the past few years, several studies have investigated data-driven controller synthesis for systems with complete state information. When the system model is unavailable, [92] offers an approach to synthesis controllers for single-input, single-output feedback linearizable systems. The result in [93] examines a data-enabled predictive control technique for linear stochastic systems for which the model is unavailable and the controller is derived from noisy input-output data. Given that an upper bound on the dimension of the system is available, [94] presents a data-driven model predictive control scheme solely based on initially measured input-output data. By collecting input-output data over a finite time horizon, [95] proposes a methodology to compute control laws for nonlinear polynomial-type systems. Using the so-called *behavioural framework*, which is a data-driven method proposed in [96], state and output feedback stabilization and linear quadratic regulation (LQR) problems are studied in [97]. Based on the same behavioural idea, the problem is extended to stabilizing polynomial-type systems [98], switched linear systems [99], and linear time-varying systems [100].

Barrier-based data-driven techniques, in which barrier functions are constructed directly from data, have also been investigated recently. In this respect, the result in [101] offers a data-driven verification strategy via barrier functions for stochastic systems with unknown dynamics as well as a probabilistic confidence over the verification. The extension of [101] from verification to synthesis of safety controllers is proposed in [102]. Under a certain rank condition, [103] provides a data-driven controller synthesis methodology for continuous-time nonlinear polynomial-type systems based on a single trajectory acquired from the system.

6.1.2 Contribution

The contents of this chapter have been published in the IFAC World Congress [104]. It is a joint work with Prof. Majid Zamani. The author of the thesis has established the results and written the draft. Majid Zamani supervised the work.

The main contribution of this chapter is to provide a data-driven framework for the synthesis of safety controllers for partially-observable continuous-time polynomial-type systems with unknown models. Given an appropriate estimator with a known estimation accuracy, we provide sufficient conditions for so-called *control barrier functions* under which the safety of the unknown system can be guaranteed. The control barrier function and its corresponding polynomial-type safety controller are constructed purely from data. Under a certain rank condition, which is linked to the condition of *persistency of excitation* [105], only a single state trajectory from the estimator and a single input-output trajectory from the system over a finite time horizon are needed in our setting. We illustrated our proposed results on a partially-observable jet engine example.

6.2 Preliminaries and Problem Definition

For the PO-ct-PS $\mathcal{S}_P$ as in (2.3.3), we assume matrices $\mathcal{A}, \mathcal{B}$, and $\mathcal{C}$ are unknown and we employ the term *unknown model* to refer to this type of system. Furthermore, we raise the following assumption on the existence of an estimator that can estimate the states of $\mathcal{S}_P$ with an upper bound on the estimation accuracy.

Assumption 8. *Consider a PO-ct-PS $\mathcal{S}_P$ as in* (2.3.3)*. States of $\mathcal{S}_P$ can be estimated by a proper estimator $\widehat{\mathcal{S}}_P$ represented as:*

$$\widehat{\mathcal{S}}_P : \begin{cases} \dot{\hat{x}} = \mathcal{A}\mathcal{M}(\hat{x}) + \mathcal{B}u + K\big(\mathcal{C}\mathcal{M}(x) - \mathcal{C}\mathcal{M}(\hat{x})\big), \\ \hat{y} = \mathcal{C}\mathcal{M}(\hat{x}), \end{cases} \tag{6.2.1}$$

with $\hat{x} \in \widehat{X}$ and $\hat{y} \in \widehat{Y}$, where $\widehat{X} \subset \mathbb{R}^n$ and $\widehat{Y} \subset \mathbb{R}^p$ are the estimator's state and output set, respectively. Furthermore, $X \subseteq \widehat{X}$ and $Y \subseteq \widehat{Y}$. The matrix $K \in \mathbb{R}^{n\times p}$ is the known estimator gain, and $\mathcal{A}, \mathcal{B}$, and $\mathcal{C}$ are the unknown matrices as in $\mathcal{S}_P$. Moreover, in this chapter, we consider a guaranteed upper bound on the estimation accuracy as:

$$\|x(t) - \hat{x}(t)\| \leq \epsilon, \quad \forall t \in \mathbb{R}_{\geq 0}, \tag{6.2.2}$$

where $\epsilon \in \mathbb{R}_{>0}$ is a known constant.

Now we can formally define the main synthesis problem that we are interested in solving in this chapter.

Problem 57. *Consider a PO-ct-PS $\mathcal{S}_P$ as in* (2.3.3) *with unknown matrices $\mathcal{A}, \mathcal{B}$, and $\mathcal{C}$, its estimator $\widehat{\mathcal{S}}_P$ as in* (6.2.1) *with the estimation accuracy ϵ as in* (6.2.2)*. Let $X_0, X_1 \subset X$ represent initial and unsafe sets for $\mathcal{S}_P$, respectively. Synthesize a polynomial-type safety controller using which the trajectories of $\mathcal{S}_P$ starting from initial set X_0 never reach the unsafe set X_1.*

To synthesize a controller for Problem 57, we utilize a notion of *control barrier functions*, introduced in the next section.

6.3 Control Barrier Functions

In this section, we define a notion of control barrier functions (CBFs), adopted from [15], as formalized in the following definition.

Definition 58. *Consider a PO-ct-PS $\mathcal{S}_P$ as in* (2.3.3)*, its estimator $\widehat{\mathcal{S}}_P$ as in* (6.2.1) *together with an estimation accuracy ϵ as in* (6.2.2)*, and $X_0, X_1 \subset X \subseteq \widehat{X}$ as initial and unsafe sets of $\mathcal{S}_P$, respectively. Let us define $X_1^\epsilon \subset \widehat{X}$ as an ϵ-inflated version of X_1. A function $\mathcal{B} : \widehat{X} \to \mathbb{R}$ is called a control barrier function for $\widehat{\mathcal{S}}_P$ if there exists constants $\beta_0, \beta_1 \in \mathbb{R}$, with $\beta_0 < \beta_1$, such that*

- $\forall \hat{x} \in X_0$,

$$\mathcal{B}(\hat{x}) \leq \beta_0, \tag{6.3.1}$$

- $\forall \hat{x} \in X_1^\epsilon$,

$$\mathcal{B}(\hat{x}) \geq \beta_1, \tag{6.3.2}$$

- $\forall \hat{x} \in \widehat{X}, \exists u \in U$, *such that* $\forall x \in X$,

$$\mathsf{L}\mathcal{B}(x, \hat{x}, u) \leq 0, \tag{6.3.3}$$

where $\mathsf{L}\mathcal{B}$ *is the Lie derivative of* $\mathcal{B}$ *with respect to the dynamic of the estimator, which is defined as*

$$\mathsf{L}\mathcal{B}(x, \hat{x}, u) := \frac{\partial \mathcal{B}(\hat{x})}{\partial \hat{x}} \Big(\mathcal{A}\mathcal{M}(\hat{x}) + \mathcal{B}u + K\big(\mathcal{C}\mathcal{M}(x) - \mathcal{C}\mathcal{M}(\hat{x})\big)\Big). \tag{6.3.4}$$

The above definition implicitly associates a controller to a CBF according to the existential quantifier over the input for any $\hat{x} \in \widehat{X}$.

Remark 59. *Note that* X_0 *and* X_1^ϵ *should not intersect in order to enforce the safety property in Definition 58. This condition is implicitly enforced by imposing* $\beta_0 < \beta_1$.

The next theorem shows how CBFs can be used in order to make sure that the unknown PO-ct-PS $\mathcal{S}_P$ in (2.3.3) is safe in the sense that its trajectories starting from X_0 never reach X_1.

Theorem 60. *Let* $\mathcal{S}_P$ *be a PO-ct-PS as in* (2.3.3) *and* $\widehat{\mathcal{S}}_P$ *be its corresponding estimator as in* (6.2.1) *with the estimation accuracy* ϵ *as in* (6.2.2). *Suppose* $\mathcal{B}$ *is a CBF for* $\widehat{\mathcal{S}}_P$ *as in Definition 58. Then, one gets* $x_{x_0 v}(t) \notin X_1$ *for any* $x_0 \in X_0$ *and any* $t \in \mathbb{R}_{\geq 0}$, *where the control input* u *is chosen in such a way that* (6.3.3) *holds.*

Proof. Since $\mathsf{L}\mathcal{B}(x, \hat{x}, u)$ is non-positive, one can infer that if $\mathcal{B}(\hat{x}(0)) \leq \beta_0, \forall \hat{x}(0) \in X_0$, then $\mathcal{B}(\hat{x}(t)) \leq \beta_0, \forall t \in \mathbb{R}_{>0}$. Now since $\beta_0 < \beta_1$, one can readily conclude that $\mathcal{B}(\hat{x}(t)) < \beta_1$. From (6.3.2), one gets $\hat{x}_{\hat{x}_0 v}(t) \notin X_1^\epsilon, \forall \hat{x}_0 \in X_0$ and $\forall t \in \mathbb{R}_{\geq 0}$. Now, by utilizing the fact that $\hat{x}$ estimates x with an upper bound on the estimation accuracy ϵ as in (6.2.2), and since X_1^ϵ is an ϵ-inflated version of X_1, one gets $x_{x_0 v}(t) \notin X_1, \forall x_0 \in X_0$ and $\forall t \in \mathbb{R}_{\geq 0}$, which concludes the proof. □

In the next section, we propose a data-driven approach in order to construct control barrier functions for unknown PO-ct-PSs as in (2.3.3).

6.4 Data-Driven Controller Synthesis via CBFs

We now provide our data-driven approach in order to synthesize safety controllers for the unknown PO-ct-PS $\mathcal{S}_P$ in (2.3.3) using its estimator $\widehat{\mathcal{S}}_P$ in (6.2.1). To do so, we first collect input-output data from the unknown PO-ct-PS $\mathcal{S}_P$ and its estimator $\widehat{\mathcal{S}}_P$ over the time interval $[t_0, t_0+(T_s-1)\Delta_t]$, where Δ_t is the sampling time, and $T_s \in \mathbb{N}_{>0}$ is the number of collected samples. Then, using the collected data from $\mathcal{S}_P$, we collect input-output data from the estimator $\widehat{\mathcal{S}}_P$. The collected samples are denoted as follows:

$$\begin{aligned}
\mathcal{U}_{0,T_s} &:= \big[u(t_0), u(t_0+\Delta_t), \cdots, u(t_0+(T_s-1)\Delta_t)\big], \\
\mathcal{Y}_{0,T_s} &:= \big[y(t_0), y(t_0+\Delta_t), \cdots, y(t_0+(T_s-1)\Delta_t)\big], \\
\widehat{\mathcal{X}}_{0,T_s} &:= \big[\hat{x}(t_0), \hat{x}(t_0+\Delta_t), \cdots, \hat{x}(t_0+(T_s-1)\Delta_t)\big], \\
\widehat{\mathcal{X}}_{1,T_s} &:= \big[\dot{\hat{x}}(t_0), \dot{\hat{x}}(t_0+\Delta_t), \cdots, \dot{\hat{x}}(t_0+(T_s-1)\Delta_t)\big].
\end{aligned} \tag{6.4.1}$$

Remark 61. *Observe that in order to construct $\widehat{\mathcal{X}}_{1,T_s}$, one needs to have access to the derivatives of the states of the estimator at sampling times. Since this data is generally not available via measurements, proposed results in the relevant literature can be utilized in order to approximate derivatives using some filters (cf. [106, 107, 108]). Although a small numerical error gets introduced from approximating the derivatives, we do not consider this error in our analysis.*

Next, we use the results of [95] in order to provide a data-based representation of the closed-loop estimator $\widehat{\mathcal{S}}_P$ in (6.2.1) using a polynomial-type safety controller of the form $\mathsf{u} = Z(\hat{x})\mathcal{M}(\hat{x})$, where the matrix polynomial $Z(\hat{x})$ is to be synthesized.

Lemma 62. *Let $F(\hat{x})$ be a $(T_s \times N)$ matrix polynomial such that*

$$\mathbb{I}_N = \widehat{\mathcal{M}}_{0,T_s} F(\hat{x}),$$

where $\widehat{\mathcal{M}}_{0,T_s}$ is an $(N \times T_s)$ full row-rank matrix constructed from the vector $\mathcal{M}(\hat{x})$ and samples $\widehat{\mathcal{X}}_{0,T_s}$ as follows

$$\widehat{\mathcal{M}}_{0,T_s} = \big[\mathcal{M}\big(\hat{x}(t_0)\big), \cdots, \mathcal{M}\big(\hat{x}(t_0+(T_s-1)\Delta_t)\big)\big].$$

If the controller is set to be as $\mathsf{u} = Z(\hat{x})\mathcal{M}(\hat{x}) = \mathcal{U}_{0,T_s} F(\hat{x})\mathcal{M}(\hat{x})$, then the data-based representation of the closed loop estimator $\dot{\hat{x}} = \mathcal{A}\mathcal{M}(\hat{x}) + \mathcal{B}u + K\big(\mathcal{C}\mathcal{M}(x) - \mathcal{C}\mathcal{M}(\hat{x})\big)$ is as follows:

$$\dot{\hat{x}} = \big(\widehat{\mathcal{X}}_{1,T_s} - K\mathcal{Y}_{0,T_s}\big) F(\hat{x})\mathcal{M}(\hat{x}) + K\mathcal{Y}_{0,T_s} F(x)\mathcal{M}(x),$$

or equivalently,

$$\mathcal{A} + \mathcal{B}Z(\hat{x}) - K\mathcal{C} = (\widehat{\mathcal{X}}_{1,T_s} - K\mathcal{Y}_{0,T_s})F(\hat{x}),$$

$$\text{and} \quad K\mathcal{C} = K\mathcal{Y}_{0,T_s} F(x).$$

Proof. Since $\mathbb{I}_N = \widehat{\mathcal{M}}_{0,T_s} F(\hat{x})$, then

$$\mathcal{C} = \mathcal{C}\widehat{\mathcal{M}}_{0,T_s} F(\hat{x}) = \widehat{\mathcal{Y}}_{0,T_s} F(\hat{x}),$$

and, accordingly, $\mathcal{C} = \mathcal{Y}_{0,T_s} F(x)$. Since $Z(\hat{x}) = \mathcal{U}_{0,T_s} F(\hat{x})$, the closed loop estimator $\widehat{\mathcal{S}}_P$ can be written as

$$\begin{aligned}\dot{\hat{x}} =& \big(\mathcal{A} + \mathcal{B}Z(\hat{x}) - K\mathcal{C}\big)\mathcal{M}(\hat{x}) + K\mathcal{C}\mathcal{M}(x)\\ =& \big(\mathcal{A}\widehat{\mathcal{M}}_{0,T_s} + \mathcal{B}\mathcal{U}_{0,T_s} - K\widehat{\mathcal{Y}}_{0,T_s}\big)F(\hat{x})\mathcal{M}(\hat{x})\\ &+ K\mathcal{Y}_{0,T_s}F(x)\mathcal{M}(x) = \big(\widehat{\mathcal{X}}_{1,T_s} - K\mathcal{Y}_{0,T_s}\big)F(\hat{x})\mathcal{M}(\hat{x})\\ &+ K\mathcal{Y}_{0,T_s}F(x)\mathcal{M}(x),\end{aligned}$$

with $\widehat{\mathcal{X}}_{1,T_s} = \mathcal{A}\widehat{\mathcal{M}}_{0,T_s} + \mathcal{B}\mathcal{U}_{0,T_s} + K\big(\mathcal{Y}_{0,T_s} - \widehat{\mathcal{Y}}_{0,T_s}\big)$. Hence, $\dot{\hat{x}} = \big(\widehat{\mathcal{X}}_{1,T_s} - K\widehat{\mathcal{Y}}_{0,T_s}\big)F(\hat{x})\mathcal{M}(\hat{x}) + K\mathcal{Y}_{0,T_s}F(x)\mathcal{M}(x)$, equivalently, $\mathcal{A} + \mathcal{B}Z(\hat{x}) - K\mathcal{C} = (\widehat{\mathcal{X}}_{1,T_s} - K\mathcal{Y}_{0,T_s})F(\hat{x})$ and $K\mathcal{C} = K\mathcal{Y}_{0,T_s}F(x)$, is the data-based representation of the closed-loop estimator $\widehat{\mathcal{S}}_P$, which completes the proof. □

Remark 63. *Note that the number of samples T_s should be at least N in order for $\widehat{\mathcal{M}}_{0,T_s}$ to have full row rank.*

The following theorem, inspired by [103, Theorem 8], shows the usefulness of CBFs in order to solve Problem 57. To do so, we construct the CBF from data and use the data-based representation in Lemma 62 in order to synthesize the controller gain $Z(\hat{x})$, such that $\mathsf{u} = Z(\hat{x})\mathcal{M}(\hat{x})$ makes the unknown PO-ct-PS (2.3.3) safe.

Theorem 64. *Let $\mathcal{S}_P$ be a PO-ct-PS in* (2.3.3) *and $\widehat{\mathcal{S}}_P$ be its estimator in* (6.2.1) *together with an estimation accuracy ϵ as in* (6.2.2)*. Suppose there exists a matrix polynomial $H(\hat{x}) \in \mathbb{R}^{T_s \times N}$ such that $\widehat{\mathcal{M}}_{0,T_s} H(\hat{x}) = \mathcal{P}^{-1}, \forall \hat{x} \in \widehat{X}$, with $\mathcal{P} \succ 0$. If conditions* (6.4.2)-(6.4.4) *are satisfied, then $\mathcal{B}(\hat{x}) = \mathcal{M}(\hat{x})^\top [\widehat{\mathcal{M}}_{0,T_s} H(\hat{x})]^{-1} \mathcal{M}(\hat{x})$ is a CBF and $\mathsf{u} = \mathcal{U}_{0,T_s} H(\hat{x}) \big(\widehat{\mathcal{M}}_{0,T_s} H(\hat{x})\big)^{-1} \mathcal{M}(\hat{x})$ is its corresponding safety controller which makes the unknown PO-ct-PS $\mathcal{S}_P$ safe:*

- $\forall \hat{x} \in X_0$,

$$\mathcal{M}(\hat{x})^\top [\widehat{\mathcal{M}}_{0,T_s} H(\hat{x})]^{-1} \mathcal{M}(\hat{x}) \leq \beta_0, \tag{6.4.2}$$

- $\forall \hat{x} \in X_1^\epsilon$,

$$\mathcal{M}(\hat{x})^\top [\widehat{\mathcal{M}}_{0,T_s} H(\hat{x})]^{-1} \mathcal{M}(\hat{x}) \geq \beta_1, \tag{6.4.3}$$

- $\forall \hat{x} \in \widehat{X}$,

$$\begin{aligned}
&\mathcal{M}(\hat{x})^\top\mathcal{P}\Big[\frac{\partial\mathcal{M}(\hat{x})}{\partial\hat{x}}(\widehat{\mathcal{X}}_{1,T_s}-K\mathcal{Y}_{0,T_s})H(\hat{x})+H(\hat{x})^\top(\widehat{\mathcal{X}}_{1,T_s}-K\mathcal{Y}_{0,T_s})^\top(\frac{\partial\mathcal{M}(\hat{x})}{\partial\hat{x}})^\top\Big]\mathcal{P}\mathcal{M}(\hat{x})\\
&+\mathcal{M}(\hat{x})^\top\mathcal{P}\Big[\frac{\partial\mathcal{M}(\hat{x})}{\partial\hat{x}}K\mathcal{Y}_{0,T_s}H(x)\Big]\mathcal{P}\mathcal{M}(x)\\
&+\mathcal{M}(x)^\top\mathcal{P}\Big[H(x)^\top(K\mathcal{Y}_{0,T_s})^\top(\frac{\partial\mathcal{M}(\hat{x})}{\partial\hat{x}})^\top\Big]\mathcal{P}\mathcal{M}(\hat{x})\leq 0,
\end{aligned}\tag{6.4.4}$$

where $\beta_0<\beta_1$, $\beta_0,\beta_1\in\mathbb{R}$.

Proof. Since $\mathcal{B}(\hat{x})=\mathcal{M}(\hat{x})^\top\mathcal{P}\mathcal{M}(\hat{x})$ and $\mathcal{P}^{-1}=\widehat{\mathcal{M}}_{0,T_s}H(\hat{x})$, it is straightforward that conditions (6.4.2) and (6.4.3) indicate (6.3.1) and (6.3.2), respectively. Now, we show that condition (6.3.3) holds as well. Considering the Lie derivative associated with the estimator $\widehat{\mathcal{S}}_P$, one has

$$\begin{aligned}
\mathsf{L}\mathcal{B}(x,\hat{x},u)&=\mathcal{M}(\hat{x})^\top\mathcal{P}\frac{\partial\mathcal{M}(\hat{x})}{\partial\hat{x}}\Big((\mathcal{A}+\mathcal{B}Z(\hat{x})-K\mathcal{C})\mathcal{M}(\hat{x})+K\mathcal{C}\mathcal{M}(x)\Big)\\
&+\Big(\mathcal{M}(x)^\top(K\mathcal{C})^\top+\mathcal{M}(\hat{x})^\top(\mathcal{A}+\mathcal{B}Z(\hat{x})-K\mathcal{C})^\top\Big)(\frac{\partial\mathcal{M}(\hat{x})}{\partial\hat{x}})^\top\mathcal{P}\mathcal{M}(\hat{x})\\
&=\mathcal{M}(\hat{x})^\top\mathcal{P}\Big[\frac{\partial\mathcal{M}(\hat{x})}{\partial\hat{x}}(\mathcal{A}+\mathcal{B}Z(\hat{x})-K\mathcal{C})\mathcal{P}^{-1}+\mathcal{P}^{-1}(\mathcal{A}+\mathcal{B}Z(\hat{x})-K\mathcal{C})^\top(\frac{\partial\mathcal{M}(\hat{x})}{\partial\hat{x}})^\top\Big]\mathcal{P}\mathcal{M}(\hat{x})\\
&+\mathcal{M}(\hat{x})^\top\mathcal{P}\Big[\frac{\partial\mathcal{M}(\hat{x})}{\partial\hat{x}}K\mathcal{C}\mathcal{P}^{-1}\Big]\mathcal{P}\mathcal{M}(x)+\mathcal{M}(x)^\top\mathcal{P}\Big[\mathcal{P}^{-1}(K\mathcal{C})^\top(\frac{\partial\mathcal{M}(\hat{x})}{\partial\hat{x}})^\top\Big]\mathcal{P}\mathcal{M}(\hat{x}).
\end{aligned}$$

Since $\mathcal{P}^{-1}=\widehat{\mathcal{M}}_{0,T_s}H(\hat{x})$, then $\mathcal{P}^{-1}\mathcal{P}=\mathbb{I}_N=\widehat{\mathcal{M}}_{0,T_s}H(\hat{x})\mathcal{P}$. Since $\mathbb{I}_N=\widehat{\mathcal{M}}_{0,T_s}F(\hat{x})$, then $F(\hat{x})=H(\hat{x})\mathcal{P}$ and, therefore, $F(\hat{x})\mathcal{P}^{-1}=H(\hat{x})$. Accordingly, one has $F(x)\mathcal{P}^{-1}=H(x)$. Then,

$$(\mathcal{A}+\mathcal{B}Z(\hat{x})-K\mathcal{C})\mathcal{P}^{-1}=(\widehat{\mathcal{X}}_{1,T_s}-K\mathcal{Y}_{0,T_s})F(\hat{x})\mathcal{P}^{-1}=(\widehat{\mathcal{X}}_{1,T_s}-K\mathcal{Y}_{0,T_s})H(\hat{x}),$$

and

$$K\mathcal{C}\mathcal{P}^{-1}=K\mathcal{Y}_{0,T_s}F(x)\mathcal{P}^{-1}=K\mathcal{Y}_{0,T_s}H(x).$$

Hence,

$$\begin{aligned}
\mathsf{L}\mathcal{B}(x,\hat{x},u)&=\mathcal{M}(\hat{x})^\top\mathcal{P}\Big[\frac{\partial\mathcal{M}(\hat{x})}{\partial\hat{x}}(\widehat{\mathcal{X}}_{1,T_s}-K\mathcal{Y}_{0,T_s})H(\hat{x})\\
&+H(\hat{x})^\top(\widehat{\mathcal{X}}_{1,T_s}-K\mathcal{Y}_{0,T_s})^\top(\frac{\partial\mathcal{M}(\hat{x})}{\partial\hat{x}})^\top\Big]\mathcal{P}\mathcal{M}(\hat{x})+\mathcal{M}(\hat{x})^\top\mathcal{P}\Big[\frac{\partial\mathcal{M}(\hat{x})}{\partial\hat{x}}K\mathcal{Y}_{0,T_s}H(x)\Big]\mathcal{P}\mathcal{M}(x)\\
&+\mathcal{M}(x)^\top\mathcal{P}\Big[H(x)^\top(K\mathcal{Y}_{0,T_s})^\top(\frac{\partial\mathcal{M}(\hat{x})}{\partial\hat{x}})^\top\Big]\mathcal{P}\mathcal{M}(\hat{x}).
\end{aligned}$$

Thus, if (6.4.4) holds, condition (6.3.3) is satisfied. Consequently,

$$\mathcal{B}(\hat{x})=\mathcal{M}(\hat{x})\big[\widehat{\mathcal{M}}_{0,T_s}H(\hat{x})\big]^{-1}\mathcal{M}(\hat{x}),$$

is a CBF and

$$\mathsf{u}=\mathcal{U}_{0,T_s}F(\hat{x})\mathcal{M}(\hat{x})=\mathcal{U}_{0,T_s}H(\hat{x})\big[\widehat{\mathcal{M}}_{0,T_s}H(\hat{x})\big]^{-1}\mathcal{M}(\hat{x}),$$

is the corresponding safety controller for the PO-ct-PS $\mathcal{S}_P$, which completes the proof. □

In the next section, we discuss the computation of the CBF defined in Definition 58.

6.5 Computation of CBFs

In this section, we provide a systematic approach to implement Theorem 64 and search for CBFs and their corresponding controllers. The proposed method is based on a sum-of-square (SOS) optimization problem [88]. To do so, we consider the state set of the system and the estimator X, $\widehat{X}$, the initial set X_0, and the unsafe set X_1^ϵ as

$$X = \bigcup_{i=1}^{n_x} X_i, X_i := \big\{x \in \mathbb{R}^n \,|\, g_{ij}(x) \geq 0, j = 1, \ldots, \ell\big\}, \tag{6.5.1}$$

$$\widehat{X} = \bigcup_{i=1}^{n_{\hat{x}}} \widehat{X}_i, \widehat{X}_i := \big\{\hat{x} \in \mathbb{R}^n \,|\, \hat{g}_{ij}(\hat{x}) \geq 0, j = 1, \ldots, \hat{\ell}\big\}, \tag{6.5.2}$$

$$X_0 = \bigcup_{i=1}^{n_{x_1}} X_{0i}, X_{0i} := \big\{\hat{x} \in \mathbb{R}^n \,|\, g_{ij}^1(\hat{x}) \geq 0, j = 1,\ldots,\ell_1\big\}, \tag{6.5.3}$$

$$X_1^\epsilon = \bigcup_{i=1}^{n_{x_2}} X_{1i}^\epsilon, X_{1i}^\epsilon := \big\{\hat{x} \in \mathbb{R}^n \,|\, g_{ij}^2(\hat{x}) \geq 0, j = 1,\ldots,\ell_2\big\}, \tag{6.5.4}$$

where $n_x, n_{\hat{x}}, n_{x_1}$, and n_{x_2} are the number of regions in $X, \widehat{X}, X_0$, and X_1^ϵ, respectively. Furthermore, $g_{ij}, \hat{g}_{ij}, g_{ij}^1$, and g_{ij}^2 are polynomial functions, with $\ell, \hat{\ell}, \ell_1$, and ℓ_2 being the number of polynomials required to characterize each region. The input set U is defined as

$$U := \big\{u \in \mathbb{R}^m \mid b_{u_j}^\top u \leq 1, \text{ with } j = 1, \ldots, \ell_u\big\}, \tag{6.5.5}$$

where $b_{u_j} \in \mathbb{R}^m$ are some constant vectors. We now present the SOS formulations in the following corollary.

Corollary 65. *Consider a PO-ct-PS $\mathcal{S}_P$ in* (2.3.3) *and its estimator $\widehat{\mathcal{S}}_P$ in* (6.2.1) *together with an estimation accuracy ϵ as in* (6.2.2)*. Let $X, \widehat{X}, X_0$, and X_1^ϵ be as in* (6.5.1)-(6.5.4)*, respectively, the input set U be as in* (6.5.5)*, and data $\mathcal{U}_{0,T_s}, \mathcal{Y}_{0,T_s}, \widehat{\mathcal{X}}_{1,T_s}$, and $\widehat{\mathcal{M}}_{0,T_s}$ be as in* (6.4.1) *and in Lemma 62, respectively. If there exist a positive definite matrix $\mathcal{P} \in \mathbb{R}^{n\times n}$, a matrix polynomial $H(\hat{x}) \in \mathbb{R}^{T_s \times N}$, and $\beta_0, \beta_1 \in \mathbb{R}$, with $\beta_0 < \beta_1$, such that the following expressions are SOS polynomials*

$$-\mathcal{M}(\hat{x})^\top \mathcal{P} \mathcal{M}(\hat{x}) - \sum_{j=1}^{\ell_1} h_{ij}^1(\hat{x}) g_{ij}^1(\hat{x}) + \beta_0, \forall i \in \{1,\ldots,n_{x_1}\}, \tag{6.5.6}$$

$$\mathcal{M}(\hat{x})^\top \mathcal{P} \mathcal{M}(\hat{x}) - \sum_{j=1}^{\ell_2} h_{ij}^2(\hat{x}) g_{ij}^2(\hat{x}) - \beta_1, \forall i \in \{1,\ldots,n_{x_2}\}, \tag{6.5.7}$$

$$
\begin{aligned}
&- \mathcal{M}(\hat{x})^\top \mathcal{P}\Big[\frac{\partial \mathcal{M}(\hat{x})}{\partial \hat{x}}(\widehat{\mathcal{X}}_{1,T_s} - K\mathcal{Y}_{0,T_s})H(\hat{x}) - H(\hat{x})^\top(\widehat{\mathcal{X}}_{1,T_s} - K\mathcal{Y}_{0,T_s})^\top(\frac{\partial \mathcal{M}(\hat{x})}{\partial \hat{x}})^\top\Big]\mathcal{P}\mathcal{M}(\hat{x}) \\
&- \mathcal{M}(\hat{x})^\top \mathcal{P}\Big[\frac{\partial \mathcal{M}(\hat{x})}{\partial \hat{x}}K\mathcal{Y}_{0,T_s}H(x)\Big]\mathcal{P}\mathcal{M}(x) - \mathcal{M}(x)^\top \mathcal{P}\Big[H(x)^\top(K\mathcal{Y}_{0,T_s})^\top(\frac{\partial \mathcal{M}(\hat{x})}{\partial \hat{x}})^\top\Big]\mathcal{P}\mathcal{M}(\hat{x}) \\
&- \sum_{j=1}^{\hat{\ell}} \hat{h}_{\hat{i}j}(\hat{x})\hat{g}_{\hat{i}j}(\hat{x}) - \sum_{j=1}^{\ell} h_{ij}(x)g_{ij}(x), \forall i \in \{1,\dots,n_x\}, \forall \hat{i} \in \{1,\dots,n_{\hat{x}}\},
\end{aligned} \tag{6.5.8}
$$

$$
1 - b_{u_j}^\top \mathcal{U}_{0,T_s}H(\hat{x})\mathcal{P}\mathcal{M}(\hat{x}) - h_u(\hat{x})\Big(\beta_0 - \mathcal{M}(\hat{x})^\top \mathcal{P}\mathcal{M}(\hat{x})\Big), \forall j \in \{1,\dots \ell_u\}, \tag{6.5.9}
$$

with $h_{ij}^1(\hat{x}), h_{ij}^2(\hat{x}), \hat{h}_{\hat{i}j}(\hat{x}), h_{ij}(x)$, and $h_u(\hat{x})$ being SOS polynomials of appropriate dimensions, then $\mathcal{B}(\hat{x}) = \mathcal{M}(\hat{x})^\top \mathcal{P}\mathcal{M}(\hat{x})$ is a CBF for $\widehat{\mathcal{S}}_P$, and $\mathsf{u} = \mathcal{U}_{0,T_s}H(\hat{x})\mathcal{P}\mathcal{M}(\hat{x})$ is a safety controller for $\mathcal{S}_P$.

Proof. It can be readily verified that if (6.5.6) holds, then one obtains

$$
\mathcal{M}(\hat{x})^\top \mathcal{P}\mathcal{M}(\hat{x}) + \sum_{j=1}^{\ell_1} h_{ij}^1(\hat{x})g_{ij}^1(\hat{x}) \leq \beta_0, \forall i \in \{1,\dots,n_1\}.
$$

Since $g_{ij}^1(\hat{x})$ is non-negative by the definition of X_0 in (6.5.3), and $\hat{h}_{ij}(\hat{x})$ is SOS polynomial, then $\sum_{j=1}^{\ell_1} h_{ij}^1(\hat{x})g_{ij}^1(\hat{x})$ is also non-negative. Thus, $\forall \hat{x} \in X_0$, one has $\mathcal{M}(\hat{x})^\top \mathcal{P}\mathcal{M}(\hat{x}) \leq \beta_0$, and (6.4.2) is satisfied with $\mathcal{P} = \Big[\widehat{\mathcal{M}}_{0,T_s}H(\hat{x})\Big]^{-1}$. In a similar way, (6.5.7) and (6.5.8), respectively, imply that (6.4.3) and (6.4.4) hold with $\mathcal{P} = \Big[\widehat{\mathcal{M}}_{0,T_s}H(\hat{x})\Big]^{-1}$. Finally, we show that (6.5.9) ensures that $\mathsf{u} = \mathcal{U}_{0,T_s}H(\hat{x})\mathcal{P}\mathcal{M}(\hat{x}) \in U$, $\forall \hat{x} \in \widehat{X}_{\beta_0}$ with $\widehat{X}_{\beta_0} := \big\{\hat{x} \in \mathbb{R}^n \mid \mathcal{M}(\hat{x})^\top \mathcal{P}\mathcal{M}(\hat{x}) \leq \beta_0\big\}$. Note that since $\mathsf{L}\mathcal{B}(x,\hat{x},u)$ is non-positive, the trajectories of the estimator stay inside the set $\widehat{X}_{\beta_0}$ and, therefore, one only needs to consider the set $\widehat{X}_{\beta_0}$ instead of the whole state set $\widehat{X}$. The definition of U in (6.5.5) requires

$$
b_{u_j}^\top \mathcal{U}_{0,T_s}H(\hat{x})\mathcal{P}\mathcal{M}(\hat{x}) \leq 1, \forall j \in \{1,\dots,\ell_u\}, \forall \hat{x} \in \widehat{X}_{\beta_0}. \tag{6.5.10}
$$

Since (6.5.9) implies

$$
b_{u_j}^\top \mathcal{U}_{0,T_s}H(\hat{x})\mathcal{P}\mathcal{M}(\hat{x}) + h_u(\hat{x})\big(\beta_0 - \mathcal{M}(\hat{x})^\top \mathcal{P}\mathcal{M}(\hat{x})\big) \leq 1, \forall j \in \{1,\dots \ell_u\},
$$

and $h_u(\hat{x})$ is SOS polynomial, thus (6.5.10) holds. This completes the proof. □

Remark 66. *Note that in order to search for the matrix polynomial $H(\cdot)$ and matrix $\mathcal{P}$ fulfilling conditions* (6.5.6)-(6.5.9)*, one can employ existing software tools in the relevant literature such as SOSTOOLS [63], in conjunction with a semidefinite programming solver, such as SeDuMi [64].*

Remark 67. *Observe that in condition* (6.5.9) *there exists a bilinearity between decision matrices* $\mathcal{P}$ *and* $H(\cdot)$*. In order to tackle this bilinear matrix inequality (BMI), one can first acquire a candidate for* $\mathcal{P}$ *derived from* (6.5.6) *and* (6.5.7)*, and then attempt to obtain an appropriate candidate for* $H(\cdot)$ *based on* (6.5.8) *and* (6.5.9)*. Another approach to resolve this problem is to utilize the proposed method in [109] in order to locally solve the BMI by linearizing it via a first-order perturbation approximation. Then, the problem reduces to solving the linearized version.*

6.6 Case Study

Here, we consider a nonlinear Moore-Greitzer jet engine model in no-stall mode [65] given by:

$$\mathcal{S}_P : \begin{cases} \dot{x}_1 = -x_2 - \frac{3}{2}x_1^2 - \frac{1}{2}x_1^3, \\ \dot{x}_2 = x_1 - u, \\ y = x_2, \end{cases} \tag{6.6.1}$$

where $x = [x_1; x_2], x_1 = \Phi - 1, x_2 = \Psi - \phi_c - 2$, Φ is the mass flow, Ψ is the pressure rise, and ϕ_c is a constant. System $\mathcal{S}_P$ in (6.6.1) is in the form of the PO-ct-PS in (2.3.3), with

$$\mathcal{A} = \begin{bmatrix} 0 & -1 & -\frac{3}{2} & -\frac{1}{2} \\ 1 & 0 & 0 & 0 \end{bmatrix}, \mathcal{M}(x) = \begin{bmatrix} x_1 \\ x_2 \\ x_1^2 \\ x_1^3 \end{bmatrix},$$

$$\mathcal{B} = \begin{bmatrix} 0 \\ -1 \end{bmatrix}, \mathcal{C} = \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix}.$$

We assume that matrices $\mathcal{A}, \mathcal{B}$, and $\mathcal{C}$ are all unknown and treat the system as a black-box. Here, we consider the state set $X = [-5, 5] \times [-5, 5]$, the initial set $X_0 = [-1, 1] \times [-1, 1]$, the unsafe set $X_1 = [-4.7, 4.7] \times [2, 4.7]$, and the input set $U = [-5, 5]$. Here, we consider a partially-unknown estimator as in (6.2.1) with unknown $\mathcal{A}, \mathcal{B}$, and $\mathcal{C}$ matrices and a known gain matrix as $K = [0.06738; 0.09959]$. Note that we are not providing the design procedure of the estimator. Furthermore, we compute the estimator's accuracy empirically using the results of [110] and a sufficiently large amount of data. Now with the estimator's state set as $\widehat{X} = X$ and an estimation accuracy as $\epsilon = 0.3$, we illustrate the results in Theorem 64. To do so, we collect data in the form of (6.4.1), with a sampling time of $\Delta_t = 0.01s$, and the number of samples as $T_s = 10$. With the help of Corollary 65, we obtain

$$\mathcal{P} = \begin{bmatrix} 1.212 & 0 & 0 & 0 \\ 0 & 141.5 & -1.067 & 0 \\ 0 & -1.067 & 2.511 & 0 \\ 0 & 0 & 0 & 2.172 \times 10^{-9} \end{bmatrix},$$

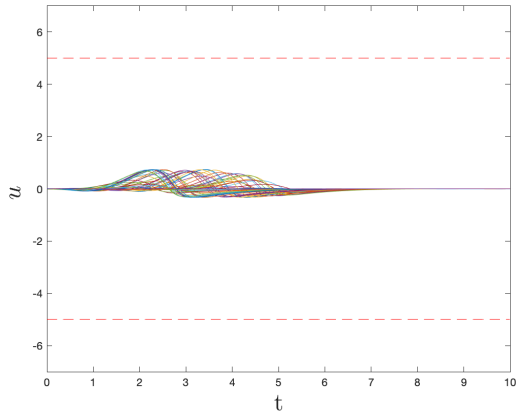

Figure 6.1: Input trajectories of the system starting from different initial conditions.

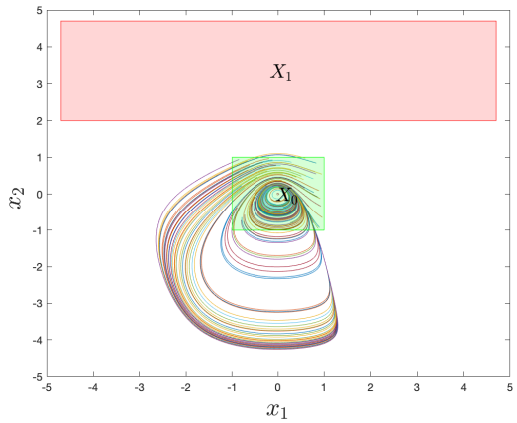

Figure 6.2: A few closed-loop state trajectories starting from different initial conditions in X_0 under controller (6.6.2).

with $\beta_0 = 150, \beta_1 = 400$, and the safety controller as follows:

$$\begin{aligned}\mathsf{u} =& 0.0011\hat{x}_1^3\hat{x}_2 - 0.0211\hat{x}_1^3 + 0.00011\hat{x}_1^2\hat{x}_2^2 - 0.0007\hat{x}_1^2\hat{x}_2 - 0.0610\hat{x}_1\hat{x}_2^2 \\ & - 0.0006\hat{x}_1\hat{x}_2 + 0.0943\hat{x}_1 - 0.0075\hat{x}_2^3 + 0.0083\hat{x}_2.\end{aligned} \tag{6.6.2}$$

For the simulation results, we initialized the system and the estimator with 100 random initial states from the initial state set and simulated the closed-loop system under the controller (6.6.2). The input and state trajectories of the system are illustrated in Figure 6.1 and Figure 6.2, respectively.

6.7 Summary

In this chapter, we established a data-driven method for the synthesis of safety controllers for partially-observable continuous-time polynomial-type systems with unknown models. Given a partially-unknown polynomial-type estimator with an upper bound on the estimation accuracy, control barrier functions were utilized in order to synthesize safety controllers. The controller associated with the control barrier function (if existing) makes the system safe. Our proposed framework only requires a single state trajectory collected from the estimator and a single output trajectory of the system, given that a specified rank condition is met. Finally, we used a case study to demonstrate the effectiveness of our proposed results.

Chapter 7

Conclusions and Future Directions

7.1 Conclusions

In this thesis, we discussed the synthesis of controllers for various classes of partially-observable cyber-physical systems. Using control barrier functions, we tackled the challenges that arise in synthesizing CPSs when full state information is not available. We conclude the thesis by reviewing the results presented in the previous chapters.

In Chapter 3, we synthesized controllers for partially-observable continuous-time stochastic control systems subjected to noisy measurements. This was accomplished through the utilization of control barrier functions. Given an estimator with a probabilistic guarantee on the accuracy of the estimation, we outlined an approach to synthesize a controller that provides a lower bound on the probability that the trajectories of the partially-observable stochastic control system remain safe over a finite time-horizon. Additionally, stochastic simulation functions were utilized to obtain the probability bound for the accuracy of the estimation.

In Chapter 4, we focused on the formal synthesis of controllers for partially-observable continuous-time jump-diffusion systems against complex logic specifications. Given a state estimator, control barrier functions were utilized in order to compute a controller together with a lower bound on the probability of satisfying complex logic specifications encoded as deterministic finite automata. By constructing control barrier functions over an augmented system consisting of the system and the estimator, the approach presented in Chapter 4 does not require prior knowledge of the estimation accuracy, which is a requirement in the results proposed in Chapter 3.

To mitigate the computational burden associated with implementing the findings presented in the preceding chapters, Chapter 5 proposed a compositional approach to synthesize networks of partially-observable discrete-time stochastic control systems. It should be noted that while the barrier-based approaches outlined in Chapters 3 and 4 demonstrate great potential, difficulties arise when attempting to apply these methods to larger partially-observable systems. In Chapter 5, we provided a compositional approach based on control barrier functions for the synthesis of safety controllers for networks of partially-

observable Markov decision processes (POMDPs) by utilizing a small-gain type reasoning. This approach involved breaking down the partially-observable large-scale interconnected stochastic control system into smaller subsystems and computing so-called local control barrier functions for subsystems. Then, the control barrier function for the interconnected system was constructed by composing the local control barrier functions. The proposed scheme provided an upper bound on the probability of the interconnected system reaching an unsafe region within a finite-time horizon. Two approaches, based on the findings in Chapters 3 and 4, were employed to construct local control barrier functions. In the first method, local control barrier functions were defined over an augmented system consisting of the subsystems and their estimators. This approach allowed for the search of local control barrier functions without prior knowledge of the estimation accuracy. The second method focused on formulating local control barrier functions solely over the estimator's dynamics, utilizing a given probability bound on the estimation accuracy, which was computed via stochastic simulation functions.

The approaches discussed in Chapters 3-5 require precise mathematical models of the systems. Therefore, it is not possible to synthesize controllers for complex systems with unknown models using these model-based methodologies. Motivated by the fact that obtaining an accurate model for many physical systems can be very challenging and computationally expensive, a data-driven scheme was proposed in Chapter 6 to synthesize safety controllers for partially-observable continuous-time polynomial-type systems with unknown dynamics. In particular, utilizing a continuous-time polynomial-type estimator with a partially-unknown dynamic and a known upper bound on estimation accuracy, Chapter 6 provided a data-driven method to compute a polynomial-type controller that guarantees the safety of the system. The proposed framework relied on control barrier functions and required only a single output trajectory from the system and a single state trajectory from its estimator.

7.2 Future Directions

In this section, we explore interesting topics that could be considered as potential future research directions.

- **Synthesis against more complex specifications.** In this thesis, our focus primarily revolved around safety specifications. Given initial and unsafe sets for partially-observable CPSs, we computed controllers ensuring that the trajectories of the systems, starting from the initial region under the synthesized controllers, will never reach the unsafe region. For stochastic systems, we also provided lower bounds on the probabilities of safety over finite time-horizons. As a potential future direction, it would be worthwhile to investigate more complex properties, such as reachability, reach-avoidance, and temporal logic specifications, in the context of partially-observable systems.

- **Neural network control barrier functions.** Another promising future direction is to explore the use of neural networks to learn control barrier functions and their corresponding controllers. Particularly, in the case of partially-observable systems, estimators can also be implemented as neural networks. This integrated approach leverages the representational power of neural networks to simultaneously learn control barrier functions, controllers, and estimators. Furthermore, the data-driven nature of neural network training can make it particularly suitable for implementing this method in the context of partially-observable systems with known mathematical models.

- **New compositionality conditions.** In Chapter 5, we utilized small-gain type reasoning to compositionally construct control barrier functions for networks of POMDPs using local control barrier functions computed for subsystems. Another possible avenue for expansion entails the development of dissipativity-type compositional conditions to construct control barrier functions for partially-observable interconnected systems based on local control barrier functions of subsystems. The utilization of the dissipativity-type compositional approach offers advantages in terms of leveraging the structure of the interconnection topology and potentially eliminating the need for imposing constraints on the gains of the subsystems [111].

- **Data-driven synthesis in other classes of partially-observable CPSs.** In Chapter 6, we presented a data-driven framework aimed at synthesizing safety controllers for partially-observable polynomial-type systems with unknown dynamics. Specifically, our approach focused on systems where the polynomial coefficients were unknown parameters. The framework relied on estimators with partially unknown dynamics, assuming knowledge of the estimator's gain. Under suitable conditions, we provided sufficient conditions for control barrier functions to ensure the safety of the unknown system. It would be interesting to investigate the synthesis problem for a broader class of partially-observable systems with unknown models. Particularly, considering scenarios where both the system model and the estimator are unknown would be of great interest. In such cases, the challenge lies in developing methodologies that can effectively synthesize controllers without relying on prior knowledge of the underlying system dynamics or the estimator model.

Bibliography

[1] Niloofar Jahanshahi, Nader Meskin, Farzaneh Abdollahi, and Wassim M Haddad. An adaptive sliding mode observer for linear systems under malicious attack. In *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, pages 001437–001442. IEEE, 2016.

[2] Paul Bogdan and Radu Marculescu. Towards a science of cyber-physical systems design. In *2011 IEEE/ACM Second international conference on cyber-physical systems*, pages 99–108. IEEE, 2011.

[3] Dimitrios Serpanos. The cyber-physical systems revolution. *Computer*, 51(3):70–73, 2018.

[4] Christel Baier and Joost-Pieter Katoen. *Principles of model checking*. MIT press, 2008.

[5] Vittorio De Iuliis, Giovanni Domenico Di Girolamo, Francesco Smarra, and Alessandro D'Innocenzo. A comparison of classical identification and learning-based techniques for cyber-physical systems. In *2021 29th Mediterranean conference on control and automation (MED)*, pages 179–185. IEEE, 2021.

[6] Paulo Tabuada. *Verification and control of hybrid systems: a symbolic approach*. Springer Science & Business Media, 2009.

[7] C. Belta, B. Yordanov, and E. A. Gol. *Formal methods for discrete-time dynamical systems*, volume 89. Springer, 2017.

[8] John Lygeros et al. *Hierarchical, hybrid control of large scale systems*. PhD thesis, Citeseer, 1996.

[9] S. Soudjani, A. Abate, and R. Majumdar. Dynamic Bayesian networks for formal verification of structured stochastic processes. *Acta Informatica*, 54(2):217–242, 2017.

[10] A. Lavaei, S. Soudjani, and M. Zamani. Compositional construction of infinite abstractions for networks of stochastic control systems. *Automatica*, 107:125–137, 2019.

[11] Abdalla Swikir and Majid Zamani. Compositional synthesis of finite abstractions for networks of systems: A small-gain approach. *Automatica*, 107:551–561, 2019.

[12] Aaron D Ames, Xiangru Xu, Jessy W Grizzle, and Paulo Tabuada. Control barrier function based quadratic programs for safety critical systems. *IEEE Transactions on Automatic Control*, 62(8):3861–3876, 2016.

[13] Pushpak Jagtap, Sadegh Soudjani, and Majid Zamani. Formal synthesis of stochastic systems via control barrier certificates. *arXiv preprint arXiv:1905.04585*, 2019.

[14] Pushpak Jagtap, Abdalla Swikir, and Majid Zamani. Compositional construction of control barrier functions for interconnected control systems. In *Proceedings of the 23rd International Conference on Hybrid Systems: Computation and Control*, pages 1–11, 2020.

[15] Stephen Prajna, Ali Jadbabaie, and George J Pappas. A framework for worst-case and stochastic safety verification using barrier certificates. *IEEE Transactions on Automatic Control*, 52(8):1415–1428, 2007.

[16] Andrew Clark. Control barrier functions for complete and incomplete information stochastic systems. In *2019 American Control Conference (ACC)*, pages 2928–2935. IEEE, 2019.

[17] Andrew Clark. Control barrier functions for stochastic systems. *Automatica*, 130:109688, 2021.

[18] B Øksendal. *Stochastic Differential Equations: An Introduction with Applications*. Springer-Verlag, Berlin, 2000.

[19] I Karatzsas and Steven E Shreve. Brownian motion and stochastic calculus. *Graduate texts in Mathematics*, 113, 1991.

[20] Bernt Øksendal and Agnes Sulem. *Applied stochastic control of jump diffusions*. Springer Science & Business Media, 2007.

[21] Richard Serfozo. *Basics of applied stochastic processes*. Springer Science & Business Media, 2009.

[22] Antoine Girard, Gregor Gössler, and Sebti Mouelhi. Safety controller synthesis for incrementally stable switched systems using multiscale symbolic models. *IEEE Transactions on Automatic Control*, 61(6):1537–1549, 2015.

[23] A. D. Ames, S. Coogan, M. Egerstedt, G. Notomista, K. Sreenath, and P. Tabuada. Control barrier functions: Theory and applications. In *2019 18th European Control Conference (ECC)*, pages 3420–3431, June 2019.

[24] Aaron D Ames, Jessy W Grizzle, and Paulo Tabuada. Control barrier function based quadratic programs with application to adaptive cruise control. In *53rd IEEE Conference on Decision and Control*, pages 6271–6278. IEEE, 2014.

[25] Mahathi Anand, Pushpak Jagtap, and Majid Zamani. Verification of switched stochastic systems via barrier certificates. In *2019 IEEE 58th Conference on Decision and Control (CDC)*, pages 4373–4378. IEEE, 2019.

[26] Chao Huang, Xin Chen, Wang Lin, Zhengfeng Yang, and Xuandong Li. Probabilistic safety verification of stochastic hybrid systems using barrier certificates. *ACM Transactions on Embedded Computing Systems (TECS)*, 16(5s):1–19, 2017.

[27] Mohamadreza Ahmadi, Andrew Singletary, Joel W Burdick, and Aaron D Ames. Safe policy synthesis in multi-agent pomdps via discrete-time barrier functions. In *2019 IEEE 58th Conference on Decision and Control (CDC)*, pages 4797–4803. IEEE, 2019.

[28] Niloofar Jahanshahi, Pushpak Jagtap, and Majid Zamani. Synthesis of stochastic systems with partial information via control barrier functions. *IFAC-PapersOnLine*, 53(2):2441–2446, 2020.

[29] Agung A Julius, Antoine Girard, and George J Pappas. Approximate bisimulation for a class of stochastic hybrid systems. In *2006 American Control Conference*, pages 6–pp. IEEE, 2006.

[30] A Agung Julius and George J Pappas. Probabilistic testing for stochastic hybrid systems. In *2008 47th IEEE Conference on Decision and Control*, pages 4030–4035. IEEE, 2008.

[31] Konrad Reif, Stefan Gunther, Engin Yaz, and Rolf Unbehauen. Stochastic stability of the continuous-time extended kalman filter. *IEE Proceedings-Control Theory and Applications*, 147(1):45–52, 2000.

[32] A. A. Julius and G. J. Pappas. Approximations of stochastic hybrid systems. *IEEE Transactions on Automatic Control*, 54(6):1193–1203, 2009.

[33] Harold J Kushner. Stochastic stability and control. Technical report, Brown Univ Providence RI, 1967.

[34] Abolfazl Lavaei, Sadegh Esmaeil Zadeh Soudjani, Rupak Majumdar, and Majid Zamani. Compositional abstractions of interconnected discrete-time stochastic control systems. In *2017 IEEE 56th Annual Conference on Decision and Control (CDC)*, pages 3551–3556. IEEE, 2017.

[35] LLC Gurobi Optimization. Gurobi optimizer reference manual, 2019.

[36] R. Marti. *Multi-Start Methods*, pages 355–368. Springer US, Boston, MA, 2003.

[37] S. Gao, S. Kong, and E. M. Clarke. dReal: An SMT solver for nonlinear theories over the reals. In *International Conference on Automated Deduction*, pages 208–214. Springer, 2013.

[38] Stefan Ratschan. Efficient solving of quantified inequality constraints over the real numbers. *ACM Transactions on Computational Logic (TOCL)*, 7(4):723–748, 2006.

[39] Harold J Kushner. On the stability of stochastic dynamical systems. *Proceedings of the National Academy of Sciences*, 53(1):8–12, 1965.

[40] Johan Löfberg. Yalmip: A toolbox for modeling and optimization in matlab. In *Proceedings of the CACSD Conference*, volume 3. Taipei, Taiwan, 2004.

[41] Calin Belta, Boyan Yordanov, and Ebru Aydin Gol. Discrete-time dynamical systems. In *Formal Methods for Discrete-Time Dynamical Systems*, pages 111–118. Springer, 2017.

[42] Majid Zamani, Peyman Mohajerin Esfahani, Rupak Majumdar, Alessandro Abate, and John Lygeros. Symbolic control of stochastic systems via approximately bisimilar finite abstractions. *IEEE Transactions on Automatic Control*, 59(12):3135–3150, 2014.

[43] Majid Zamani, Ilya Tkachev, and Alessandro Abate. Towards scalable synthesis of stochastic control systems. *Discrete Event Dynamic Systems*, 27(2):341–369, 2017.

[44] Abolfazl Lavaei, Sadegh Soudjani, and Majid Zamani. Compositional (in) finite abstractions for large-scale interconnected stochastic systems. *IEEE Transactions on Automatic Control*, 2020.

[45] Tichakorn Wongpiromsarn, Ufuk Topcu, and Andrew Lamperski. Automata theory meets barrier certificates: Temporal logic verification of nonlinear systems. *IEEE Transactions on Automatic Control*, 61(11):3344–3355, 2015.

[46] Andrea Bisoffi and Dimos V Dimarogonas. A hybrid barrier certificate approach to satisfy linear temporal logic specifications. In *2018 Annual American Control Conference (ACC)*, pages 634–639. IEEE, 2018.

[47] Lars Lindemann and Dimos V Dimarogonas. Control barrier functions for signal temporal logic tasks. *IEEE control systems letters*, 3(1):96–101, 2018.

[48] Mahathi Anand, Vishnu Murali, Ashutosh Trivedi, and Majid Zamani. Formal verification of hyperproperties for control systems. In *Proceedings of the Workshop on Computation-Aware Algorithmic Design for Cyber-Physical Systems*, pages 29–30, 2021.

[49] Mahathi Anand, Vishnu Murali, Ashutosh Trivedi, and Majid Zamani. Verification of hyperproperties for uncertain dynamical systems via barrier certificates. *arXiv preprint arXiv:2105.05493*, 2021.

[50] Pushpak Jagtap, Sadegh Soudjani, and Majid Zamani. Temporal logic verification of stochastic systems using barrier certificates. In *International Symposium on Automated Technology for Verification and Analysis*, pages 177–193. Springer, 2018.

[51] Yiming Meng and Jun Liu. Sufficient conditions for robust probabilistic reach-avoid-stay specifications using stochastic lyapunov-barrier functions. In *2022 American Control Conference (ACC)*, pages 2283–2288. IEEE, 2022.

[52] Lars Lindemann, George J Pappas, and Dimos V Dimarogonas. Control barrier functions for nonholonomic systems under risk signal temporal logic specifications. In *2020 59th IEEE Conference on Decision and Control (CDC)*, pages 1422–1428. IEEE, 2020.

[53] Mohamadreza Ahmadi, Bo Wu, Hai Lin, and Ufuk Topcu. Privacy verification in pomdps via barrier certificates. In *2018 IEEE Conference on Decision and Control (CDC)*, pages 5610–5615. IEEE, 2018.

[54] Niloofar Jahanshahi, Pushpak Jagtap, and Majid Zamani. Synthesis of stochastic systems with partial information via control barrier functions. *21st IFAC World Congress*, 2020.

[55] Niloofar Jahanshahi, Pushpak Jagtap, and Majid Zamani. Synthesis of partially observed jump-diffusion systems via control barrier functions. *IEEE Control Systems Letters*, 5(1):253–258, 2020.

[56] Xiong Kai, Chunling Wei, and Liangdong Liu. Robust extended kalman filtering for nonlinear systems with stochastic uncertainties. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 40(2):399–405, 2009.

[57] Bor-Sen Chen, Wen-Hao Chen, and Hsuan-Liang Wu. Robust h_2 / h_∞ global linearization filter design for nonlinear stochastic systems. *IEEE transactions on circuits and systems I: Regular Papers*, 56(7):1441–1454, 2008.

[58] Chung-Shi Tseng. Robust fuzzy filter design for a class of nonlinear stochastic systems. *IEEE Transactions on Fuzzy Systems*, 15(2):261–274, 2007.

[59] Filippo Bonchi and Damien Pous. Checking nfa equivalence with bisimulations up to congruence. *ACM SIGPLAN Notices*, 48(1):457–468, 2013.

[60] John E Hopcroft, Rajeev Motwani, and Jeffrey D Ullman. Introduction to automata theory, languages, and computation. *Acm Sigact News*, 32(1):60–65, 2001.

[61] Giuseppe De Giacomo and Moshe Vardi. Synthesis for ltl and ldl on finite traces. In *Twenty-Fourth International Joint Conference on Artificial Intelligence*, 2015.

[62] Stuart J. Russell and Peter Norvig. *Artificial Intelligence: A Modern Approach*. Pearson Education, 2 edition, 2003.

[63] Stephen Prajna, Antonis Papachristodoulou, and Pablo A Parrilo. Introducing sostools: A general purpose sum of squares programming solver. In *Proceedings of the 41st IEEE Conference on Decision and Control, 2002.*, volume 1, pages 741–746. IEEE, 2002.

[64] Jos F Sturm. Using sedumi 1.02, a matlab toolbox for optimization over symmetric cones. *Optimization methods and software*, 11(1-4):625–653, 1999.

[65] Miroslav Krstic and Petar V Kokotovic. Lean backstepping design for a jet engine compressor model. In *Proceedings of International Conference on Control Applications*, pages 1047–1052. IEEE, 1995.

[66] Hoang-Dung Tran, Luan Viet Nguyen, Weiming Xiang, and Taylor T Johnson. Order-reduction abstractions for safety verification of high-dimensional linear systems. *Discrete Event Dynamic Systems*, 27(2):443–461, 2017.

[67] A. Lavaei, S. Soudjani, and M. Zamani. Compositional abstraction-based synthesis for networks of stochastic switched systems. *Automatica*, 114, 2020.

[68] A. Lavaei, S. Soudjani, and M. Zamani. Compositional (in)finite abstractions for large-scale interconnected stochastic systems. *IEEE Transactions on Automatic Control*, 65(12):5280–5295, 2020.

[69] A. Nejati and M. Zamani. Compositional construction of finite MDPs for continuous-time stochastic systems: A dissipativity approach. In *Proceedings of the 21st IFAC World Congress*, 2020.

[70] Abolfazl Lavaei, Sadegh Soudjani, and Majid Zamani. Compositional abstraction-based synthesis of general MDPs via approximate probabilistic relations. *Nonlinear Analysis: Hybrid Systems*, 39:100991, 2021.

[71] A. Nejati, S. Soudjani, and M. Zamani. Compositional construction of control barrier functions for networks of continuous-time stochastic systems. In *Proceedings of the 21st IFAC World Congress*, 2020.

[72] A. Nejati, S. Soudjani, and M. Zamani. Compositional construction of control barrier functions for continuous-time stochastic hybrid systems. *arXiv:2012.07296*, 2020.

[73] M. Anand, A. Lavaei, and M. Zamani. Compositional construction of control barrier certificates for large-scale interconnected stochastic systems. In *21st IFAC World Conference*, 2020.

[74] Mahathi Anand, Abolfazl Lavaei, and Majid Zamani. From small-gain theory to compositional construction of barrier certificates for large-scale stochastic systems. *arXiv preprint arXiv:2101.06916*, 2021.

[75] A. Nejati, S. Soudjani, and M. Zamani. Compositional construction of control barrier certificates for large-scale stochastic switched systems. *IEEE Control Systems Letters*, 4(4):845–850, 2020.

[76] Mohamadreza Ahmadi, Nils Jansen, Bo Wu, and Ufuk Topcu. Control theory meets pomdps: A hybrid systems approach. *IEEE Transactions on Automatic Control*, 2020.

[77] Mohamadreza Ahmadi, Murat Cubuktepe, Nils Jansen, and Ufuk Topcu. Verification of uncertain pomdps using barrier certificates. In *2018 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pages 115–122. IEEE, 2018.

[78] Mohamadreza Ahmadi, Bo Wu, Yuxin Chen, Yisong Yue, and Ufuk Topcu. Barrier certificates for assured machine teaching. In *2019 American Control Conference (ACC)*, pages 3658–3663. IEEE, 2019.

[79] Mohamadreza Ahmadi, Andrew Singletary, Joel W Burdick, and Aaron D Ames. Barrier functions for multiagent-pomdps with dtl specifications. In *2020 59th IEEE Conference on Decision and Control (CDC)*, pages 1380–1385. IEEE, 2020.

[80] Niloofar Jahanshahi, Abolfazl Lavaei, and Majid Zamani. Compositional construction of safety controllers for networks of continuous-space pomdps. *IEEE Transactions on Control of Network Systems*, 2022.

[81] Jinling Liang, Zidong Wang, and Xiaohui Liu. State estimation for coupled uncertain stochastic networks with missing measurements and time-varying delays: the discrete-time case. *IEEE Transactions on Neural Networks*, 20(5):781–793, 2009.

[82] Bo Shen, Zidong Wang, and Xiaohui Liu. Bounded h_∞ synchronization and state estimation for discrete time-varying stochastic complex for discrete time-varying stochastic complex networks over a finite horizon. 2011.

[83] Tong Wang, Yongsheng Ding, Lei Zhang, and Kuangrong Hao. Robust state estimation for discrete-time stochastic genetic regulatory networks with probabilistic measurement delays. *Neurocomputing*, 111:1–12, 2013.

[84] Srdjan S Stanković, Miloš S Stanković, and Dušan M Stipanović. Consensus based overlapping decentralized estimation with missing observations and communication faults. *Automatica*, 45(6):1397–1406, 2009.

[85] S. Dashkovskiy, B. S. Rüffer, and F. R. Wirth. An ISS small gain theorem for general networks. *Mathematics of Control, Signals, and Systems (MCSS)*, 19(2):93–122, 2007.

[86] Sergey N Dashkovskiy, Björn S Rüffer, and Fabian R Wirth. Small gain theorems for large scale systems and construction of ISS Lyapunov functions. *SIAM Journal on Control and Optimization*, 48(6):4089–4118, 2010.

[87] Björn S Rüffer. Monotone inequalities, dynamical systems, and paths in the positive orthant of euclidean n-space. *Positivity*, 14(2):257–283, 2010.

[88] Pablo A Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Mathematical programming*, 96(2):293–320, 2003.

[89] S. Sadraddini, S. Sivaranjani, V. Gupta, and C. Belta. Provably safe cruise control of vehicular platoons. *IEEE Control Systems Letters*, 1(2):262–267, 2017.

[90] Niloofar Jahanshahi and Riccardo MG Ferrari. Attack detection and estimation in cooperative vehicles platoons: A sliding mode observer approach. *IFAC-PapersOnLine*, 51(23):212–217, 2018.

[91] Zhong-Sheng Hou and Zhuo Wang. From model-based control to data-driven control: Survey, classification and perspective. *Information Sciences*, 235:3–35, 2013.

[92] Lucas Fraile, Matteo Marchi, and Paulo Tabuada. Data-driven stabilization of siso feedback linearizable systems. *arXiv preprint arXiv:2003.14240*, 2020.

[93] Jeremy Coulson, John Lygeros, and Florian Dörfler. Regularized and distributionally robust data-enabled predictive control. In *2019 IEEE 58th Conference on Decision and Control (CDC)*, pages 2696–2701. IEEE, 2019.

[94] Jeremy Coulson, John Lygeros, and Florian Dorfler. Distributionally robust chance constrained data-enabled predictive control. *IEEE Transactions on Automatic Control*, 2021.

[95] Meichen Guo, Claudio De Persis, and Pietro Tesi. Learning control for polynomial systems using sum of squares relaxations. In *2020 59th IEEE Conference on Decision and Control (CDC)*, pages 2436–2441. IEEE, 2020.

[96] Jan C Willems and Jan W Polderman. *Introduction to mathematical systems theory: a behavioral approach*, volume 26. Springer Science & Business Media, 1997.

[97] Claudio De Persis and Pietro Tesi. Formulas for data-driven control: Stabilization, optimality, and robustness. *IEEE Transactions on Automatic Control*, 65(3):909–924, 2019.

[98] Peyman Mohajerin Esfahani, Tobias Sutter, and John Lygeros. Performance bounds for the scenario approach and an extension to a class of non-convex programs. *IEEE Transactions on Automatic Control*, 60(1):46–58, 2014.

[99] Monica Rotulo, Claudio De Persis, and Pietro Tesi. Online learning of data-driven controllers for unknown switched linear systems. *Automatica*, 145:110519, 2022.

[100] Benita Nortmann and Thulasi Mylvaganam. Data-driven control of linear time-varying systems. In *2020 59th IEEE Conference on Decision and Control (CDC)*, pages 3939–3944. IEEE, 2020.

[101] Ali Salamati and Majid Zamani. Data-driven safety verification of stochastic systems via barrier certificates: A wait-and-judge approach. In *Learning for Dynamics and Control Conference*, pages 441–452. PMLR, 2022.

[102] Ali Salamati, Abolfazl Lavaei, Sadegh Soudjani, and Majid Zamani. Data-driven verification and synthesis of stochastic systems through barrier certificates. *arXiv preprint arXiv:2111.10330*, 2021.

[103] Ameneh Nejati, Bingzhuo Zhong, Marco Caccamo, and Majid Zamani. Data-driven controller synthesis of unknown nonlinear polynomial systems via control barrier certificates. In *Learning for Dynamics and Control Conference*, pages 763–776. PMLR, 2022.

[104] Niloofar Jahanshahi and Majid Zamani. Synthesis of controllers for partially-observable systems: A data-driven approach. *IFAC-PapersOnLine*, 2023.

[105] Jan C Willems, Paolo Rapisarda, Ivan Markovsky, and Bart LM De Moor. A note on persistency of excitation. *Systems & Control Letters*, 54(4):325–329, 2005.

[106] Alberto Padoan and Alessandro Astolfi. Towards deterministic subspace identification for autonomous nonlinear systems. In *2015 54th IEEE Conference on Decision and Control (CDC)*, pages 127–132. IEEE, 2015.

[107] Hugues Garnier, Liuping Wang, and Peter C Young. Direct identification of continuous-time models from sampled data: Issues, basic solutions and relevance. In *Identification of continuous-time models from sampled data*, pages 1–29. Springer, 2008.

[108] Hugues Garnier, Michel Mensler, and Alain Richard. Continuous-time model identification from sampled data: implementation issues and performance evaluation. *International journal of Control*, 76(13):1337–1357, 2003.

[109] Arash Hassibi, Jonathan How, and Stephen Boyd. A path-following method for solving bmi problems in control. In *Proceedings of the 1999 American control conference (Cat. No. 99CH36251)*, volume 2, pages 1385–1389. IEEE, 1999.

[110] Matteo Marchi, Jonathan Bunton, Bahman Gharesifard, and Paulo Tabuada. Safety and stability guarantees for control loops with deep learning perception. *IEEE Control Systems Letters*, 6:1286–1291, 2021.

[111] Ameneh Nejati and Majid Zamani. From dissipativity theory to compositional construction of control barrier certificates. *Leibniz Transactions on Embedded Systems*, 8(2):06–1, 2022.